TURUN YLIOPISTO

Information and Communication Technology
Cryptography

Cryptocurrencies in the Digital Age: A Holistic Examination of Technology and Trends

Intikhab Alam

Master of Science Thesis
February 2024.

Supervisor:
Prof. Ion Petre (PhD)

DEPARTMENT OF MATHEMATICS AND STATISTICS

UNIVERSITY OF TURKU
Department of Mathematics and Statistics

Intikhab Alam: Information and Communication Technology Cryptography
Master of Science Thesis , 47 Pages.
February 2024.

This thesis explores the complex world of blockchain technology and cryptocurrencies, offering an investigation of their social effects, economic ramifications, and technical underpinnings. In the introduction, the nature and hypothesis of cryptocurrencies are explained, along with their inherent advantages and disadvantages, as well as the current issues that the industry is facing. The main objective of this thesis is to advance a more logical understanding of the complex interactions among blockchain technology, cryptographic ideas, and the larger field of digital currency. A foundational approach is perceived by the mathematical preliminaries part, which clarifies important cryptographic ideas like symmetric and public-key cryptography, cryptographic protocols, cryptanalysis, and how they relate to blockchain technology.

In doing so, the thesis establishes the foundation for evaluating the complexities associated with protecting and authenticating transactions in decentralized systems. As I move on, the investigation of blockchain technology includes a review of its design, workings, and uses in various sectors of the economy. The scalability and performance issues that blockchain is facing are assessed in this section, especially considering its expanding applications. The concluding segment explores the wider ramifications of cryptocurrencies on society, summarizing their influence on society and the dynamic regulatory environment. The dynamic world of cryptocurrencies and tokens, as well as their technological foundations, economic factors, adoption trends, legal frameworks, and the crucial problem of energy consumption from mining operations, are addressed. The thesis's final remarks provide a succinct overview of the major discoveries and their possible implications for advancing blockchain technology and cryptocurrencies in the future. They also synthesize the insights obtained throughout the thesis.

Keywords: Blockchain technology, Cryptography, Cryptocurrency, Encryption, Security.

Contents

1 Introduction

In October 2008, a document was published by a person who wrote his name as Satoshi Nakamoto on his white paper. He suggested how the current physical banking system can be replaced with bitcoin currency (a cryptocurrency) [63]. The author argued that currently, our bank is maintaining records of all the transactions by a centralized system and making sure that the transaction is successful, but we can choose an alternative for it, and that is the exercise of cryptocurrency. Hence it was determined after study that cryptocurrencies are a type of digital currency that implements cryptography to secure and verify transactions as well as to regulate the creation of new units. The unseen author, Satoshi clarified that they are decentralized, which means a centralized authority or government does not control them, and they operate on a peer-to-peer network. A blockchain is a distributed ledger system that records and stores every transaction made in the network, as used by cryptocurrencies. Each transaction is verified and added to the blockchain via mining, a complex mathematical process that requires powerful computers to solve mathematical equations. Bitcoin, Ethereum, Litecoin, and Ripple are among the most popular cryptocurrencies, but there are many others in circulation [79].

Some of the prime advantages of cryptocurrencies which have grown in popularity in recent years due to their ability to provide anonymity, security, and high returns on investments. It tells us that they can be purchased and sold on various online exchanges and are frequently used as payment for goods and services. They are, however, volatile and risky because their value can fluctuate rapidly, and they are not backed by any government or financial institution. It also sheds light on its disadvantages which entail the challenges cryptocurrencies coped with are their volatility, regulation, security, usability, and energy consumption. The goal of my thesis is to explore the technical and mathematical aspects of cryptocurrencies which constitute the use of blockchain technology, cryptography, and mining. We will further analyse how these aspects affect the security, scalability, and performance of cryptocurrencies. The thesis is structured in a range from technical aspects to economic and societal aspects which give a deep insight into the currency itself and will give proposed solutions to the problems it entails in general.

2 Mathematical Preliminaries

I shall examine the basic ideas of cryptography in the following sections covering several topics that are essential to safe communication and data security. I hope to provide a thorough grasp of the mathematical underpinnings of cryptography by arranging the issues in an organised way. The following essential elements will be covered throughout the conversation: An introduction to cryptography that provides background information for later topics.

- *Encryption*: An investigation into encryption techniques, the transformation of data into a safe format to stop unwanted access;
- *Private Key in Symmetric Key Cryptography*;
- *Data Encryption Standards (DES)*: Analysing the widely-used data encryption standard;
- *Advanced Encryption Standard (AES):*The strong encryption standard that is frequently used for secure communication;
- *Blowfish:* Comprehending the cryptographic importance of the Blowfish algorithm;
- *Public Key Encryption*;
- *RSA (Rivest-Shamir-Adleman):* Examining the inner workings of this public essential cryptography technique;
- *DSA (Digital Signature Algorithm):* Talks about the data integrity-ensuring digital signature algorithm;
- *Cryptanalysis:*A racing against the protection of encrypted data.

2.1 Cryptography

A communication engineer's specific goal is to ensure that the message that is heading to the destination from a source is the same message upon reaching [56]. The noise is an impediment or an eavesdropper. A cryptographer, on the other hand, has two goals: secrecy and authenticity. Instead, he/she may seek to ensure that the transceiver can indisputably verify the sender's identity and the message's integrity - the enemy is the spoofer, who can originate or tamper with transmitted signals. It is a fairly obvious realization that secrecy and authenticity are two very different goals. The science and technique of achieving security by encoding a message to make it readable is known as cryptography [44]. Hence credit cards, banking transactions, social security numbers and there are a lot of other information are considered sensitive information that needs to be protected from robbery. To achieve the goal of successful cryptography, various encryption techniques exist that are employed to prevent information theft. New encryption techniques are discovered with the passage of time. Data encryption has become increasingly vital as technology advances wireless communication, focusing primarily on data security during the wireless connection [59]. Specifically, the core purpose of cryptography is to ensure the "CIA triad‘’ (Confidentiality, Integrity, and Availability of the data) [62].

When diving into cryptography, there are some key terms or concepts to remember, which are identified further [44]. *Plain text* is any human-language communication that can be understood by the sender, recipient, and anyone who receives the message. *Cipher text* is the result of encoding plain text with a suitable scheme or code, and it is essential to note that cipher text is a secret message. The method used to transform plain text to cipher text is known as *encryption*, and converting cipher text back to plain text is known as *decryption*. The significant aspect of encryption and decryption is deploying the key during the processes, noting that the *key* is what makes the cryptographic process secure. Figure 1 shows a simple block diagram which also identifies the terms involved in the process, as mentioned earlier.

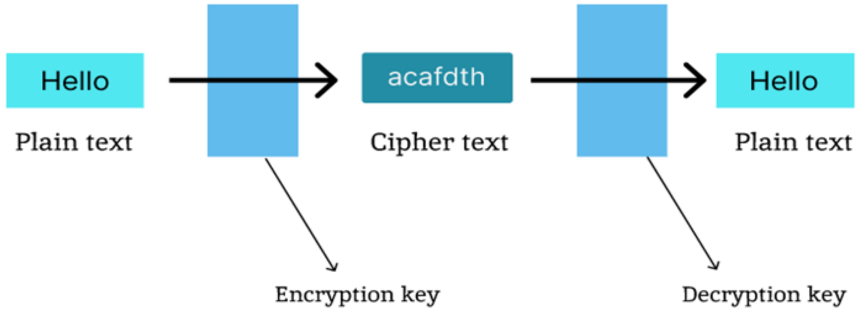


Figure 1: Encryption and decryption [1].

2.2 Encryption

Before the mid-to-late 1960s, encryption was predominantly employed for national security objectives, which remained its primary purpose. Data encryption has also been traditionally employed by inter-ministry networks, police and gendarmeries, and embassy communication systems across many nations. Only a small fraction of US-based enterprises utilised cryptographic equipment and encryption protocols[26]. Hence, it was evident that if knowledge and experience in cryptographic application were required, it would have primarily originated from the US national security community, foreign entities, and a limited number of US corporations. The development of encryption algorithms did not happen overnight, but the encryption algorithm with the best theoretical foundation was scratched in pencil on a sheet of paper. It was proposed that a random stream of characters be written onto two infinitely long tapes and sent to the parties who wish to communicate. The random stream should be added to the message by the sender and subtracted from the message by the receiver. This is the only perfect security system, but finding suppliers of infinite-length tapes proved very difficult.

Encryption is the procedure of transferring Plain Text into Cipher Text. With the support of cryptography, private messages can be sent via an unsafe channel. A key and an encryption algorithm are essential for the encryption process. The approach that has been employed in encryption is termed an encryption algorithm. Sender-side encryption takes place. The receiver-end does the decryption, which is the reverse process of encryption [77]. Since encryption has a long history stretching thousands of years, this makes it unique. Governments, military organizations, and private individuals have used encryption to shield private data from snoopers throughout history. Modern computing and communication systems depend on encryption to support safe online transactions, secure device-to-device communication, and other purposes [35].

There are several algorithms that are being used for encrypting the information. Each algorithm has a unique mathematical representation that was created after rigorous research. The block diagram in Figure 2 shows the most common algorithms in classical and advanced cryptography nowadays. I will further expand on some of these techniques, which intuitively focus on cryptocurrencies or blockchain technology. Also, I will shed light on them in terms of time and power consumption they take.

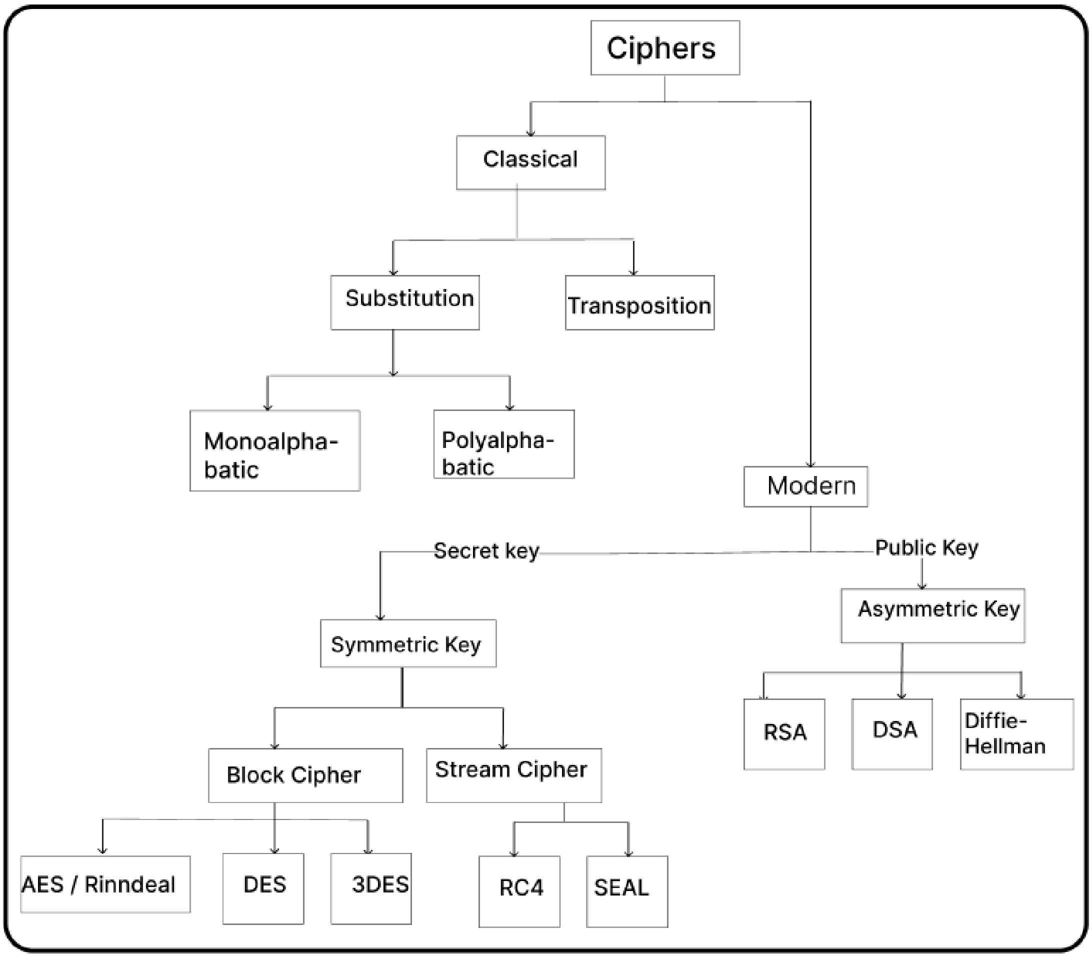


Figure 2: Classification of Encryption algorithms. [75]

Each method is effective for real-time encryption. Each technique is distinct in its own style and might be suited for a variety of applications. Fast and secure conventional encryption techniques will always operate with a high rate of security as new encryption techniques are perpetually developed [77].

2.3 Symmetric Key cryptography – Private key

A shared secret key is utilized for encoding and decrypting data by using the symmetric key encryption mechanism of cryptography. Contrary to asymmetric data encryption, symmetric encryption algorithms are much more effective at processing massive amounts of data. The functions in Stream ciphers and block ciphers, which offer bit-by-bit and block encryption, respectively, are two different types of symmetric encryption methods. Before DES (Data encryption standard) technique, there were some simple encryption methods evolved that used to be adopted for secure communication. Some of the earliest encryption techniques employed in cryptography were Simple Substitution Ciphers. Each letter in the plaintext is swapped out for a different letter or symbol in the ciphertext in these ciphers. The Atbash Cipher and the Caesar Cipher are two examples. The Caesar cipher, purportedly used by Julius Caesar during the Gallic Wars, is the most straightforward substitution cipher that is obtainable [60]. He indicated via an example that every letter in the plaintext is switched to a letter that has been pushed a certain number of positions to the right. Caesar often moved three spots. When we think of the alphabet as a cycle, the letter that comes after Z is A. As per his illustration, the table below depicts a 5-place right shift. For example
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

Note that the spaces are just for the purpose of readability, while there are no commands for including spaces. Moreover, the numbering is given from 0 until 25 in this case, as we use the numbering in the formula in the next sentences. The message “Send a signal to me” would be enciphered as “XJSI F XNLSFQ YT RJ”. The key which is generated in this case is defined by this simple equation: E(P) = (P + K) mod 26. Decryption is performed similarly as D(P) = (E − K) mod 26. It is concluded that the Caesar cipher is simple to decipher. Only 26 keys are possible, and you can test them all. When using a block cipher, every data would be divided into chunks or blocks. Data depending on block size and key is offered for the data encryption secretly. Another simple encryption way is referred to as transposition cipher. To create the ciphertext, these ciphers reorganize the letters in the plaintext. The two examples are mentioned here [24], which are the Columnar Transposition Cipher and the Rail Fence Cipher (a very simple, easy-to-crack cipher). Polyalphabetic Ciphers were found safer than simple substitution ciphers since they used several alphabets to encrypt the plaintext. The Vigenère Cipher and the Autokey Cipher are two examples. With the passage of time and observing limitations in simple breakable ciphers, more advanced techniques have evolved in SKC. Figure 2 can be seen as a tree where the branch of SKC encompasses various advanced algorithm techniques. However, some prominent and mostly used techniques are expanded in the following sections.

2.3.1 Data Encryption Standards

The first encryption standard that NIST (National Institute of Standards and Technology) announced was DES [65]. Based on their Lucifer Cipher, IBM created DES in 1972 [8]. The enciphering operation of DES was outlined as:

- DES develops a 64-bit block using data from a 64-bit long normal message and a 56-bit key;
- The bits must be adjusted in the regular text block;
- With exposure to its key permutation, the key's 8 equivalent bits are eliminated.

Then enlisted the steps for the readable message and the key generation as follows:

1. The key is first split into two halves of 28 bits each;
2. One of the halves is rotated by one or two bits depending on the round;
3. The two halves are then combined and undergo a round permutation to reduce the key from 56 bits to 48 bits, which is used to encode the round's plaintext block;
4. The rotated key halves from step 2 are used in the next round;
5. The database block is divided into two parts of 32 bits each;
6. One of the parts is expanded using permutation to increase its size to 48 bits;
7. The result of step 6 is combined with the 48-bit key from step 3 using an OR operation, and this is the only purpose of step 6;
8. The outcome of step 7 is passed through an S-box, which replaces certain key bits and reduces the 48-bit block to 32 bits;
9. The result of step 8, which is a permutation using a P-box, is combined with an OR operation;
10. The result of the P-box, which is combined with an OR operation, is used exclusively for this purpose.

The flowchart in Figure 3 visualizes the process.

2.3.2 Triple DES

3-DES is a block cipher that encrypts each data block three times using the Data Encryption Standard algorithm [76]. The 56-bit key size of the original DES encryption was no longer seen to be enough as brute-force attacks became more practical as computing power increased. 3-DES provides a means to strengthen DES's key size and thwart such cyberattacks. It relies on three 64-bit keys for a total key length of 192 bits. With Triple DES, the first key encrypts the data, the second key decrypts it and the third key re-encrypts it. Although DES is three times slower than this alternative, it promises far better protection. The decryption process is the same as the encryption process; however, it is carried out in the other direction.

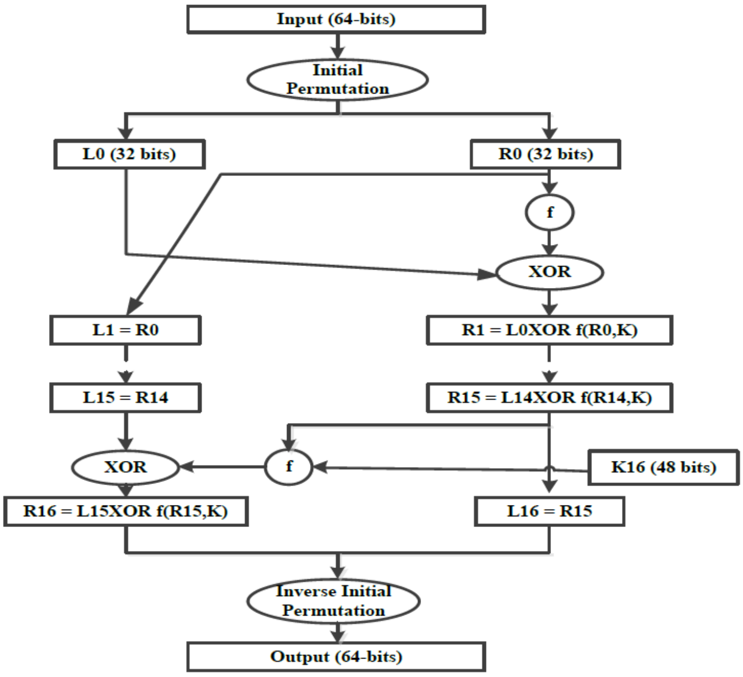


Figure 3: DES Algorithm flow chart [8]

2.3.3 Advanced Encryption Standard

NIST created the AES, a form of symmetric-key block encryption, in December 2001, which was aimed at replacing DES. It uses a non-Feistel cipher to encrypt and decrypt blocks of 128 bits [24]. This huge development is followed by a public competition launched by NIST in the late 1990s. The official news announcement came on NIST website about the winner of the global information security competition. It was reported that the competition received 15 competitor algorithms over the course of several years, which were reviewed for their performance, security, and other aspects. Five algorithms—MARS, RC6, Rijndael (pronounced "rain-dahl''), Serpent, and Twofish—were chosen as the finalists after multiple rounds of scrutiny and public discussion. After extensive scrutiny and evaluation, NIST chose Rijndael as the contest's victor in 2001. Two Belgium cryptographers, Joan Daemen (Katholieke Universiteit Leuven) and Vincent Rijmen (Provinciale Hogeschool Limburg), created Rijndael, which was renowned for integrating great performance with better security. Rijndael became among the most widespread encryption algorithms in the world after NIST defined it as AES (Advanced Encryption Standard).

Rijndael is a block cipher developed in which the number of processing rounds depends on the number of rounds and the key size (128, 192, or 256 bits) (10, 12, or 14) [70]. There are nine processing cycles if the block and key are both 128 bits. There are 11 processing rounds for a 192-bit block and key and 13 processing rounds for a 256-bit block and key [55].

The following transformations regulate each AES round [8]:

1. Byte substitution: AES uses a 128-bit data block, implying that each database entry contains 16 bytes. In sub-byte transformation, the Rijndael s-box, an 8-bit substitution box, is used to turn every bit of a data item into a different arrangement.

2. Transforming Shift Rows: This transposition is simple; based on the row position, the bytes in the remaining 3 lines of the state are cycle-shifted. A 1-byte circular left shift is executed in the second line. The third and fourth rows receive repeated two-byte and three-byte left circular shifts.

3. Mix columns transformation: In this case, the is the counterpart of a series of multiplication operations for each state's column. Every is multiplied by a stable matrix. Bytes are handled as multinames in the process.

4. Add round key transformation: This phase is done by performing an XOR between the current state's 128 bits and the round key's 128 bits. The reverse occurs in this transformation.

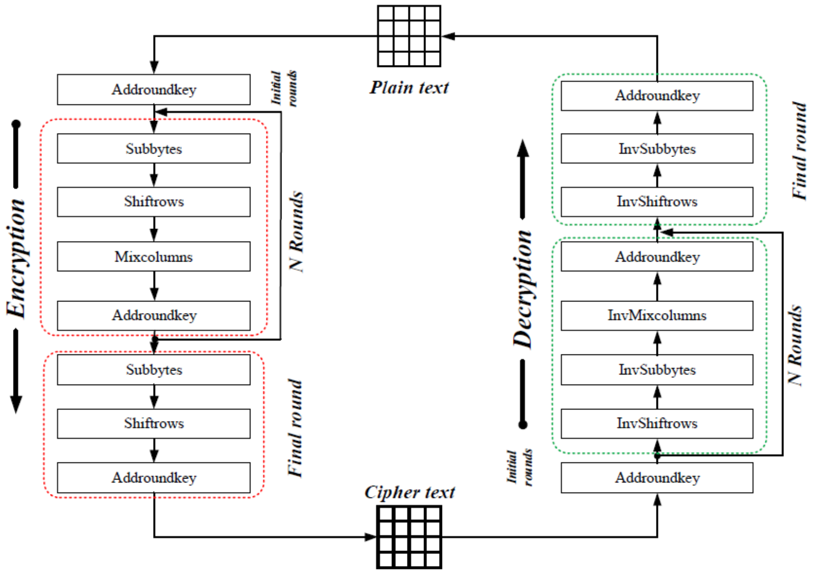


Figure 4: AES Algorithm flow chart [8].

2.3.4 Blowfish

Blowfish is a symmetric block cipher that performs well for data encryption and security. It is the perfect option for data security because it supports keys with various lengths that range from 32 to 448 bits. Bruce Schneier developed Blowfish in 1993 as a quick, cost-effective substitute for conventional encryption techniques [65]. The Feistel Network-based Blowfish algorithm iterates a straightforward encryption function 16 times. The key can be any size up to 448 bits, and the block size is

64 bits. It is significantly quicker than most cryptographic techniques when utilized on 32-bit microprocessors with big data caches. A key expansion part and a data encryption part make up the algorithm. A key of up to 448 bits can be expanded into several subkey arrays totalling 4168 bytes in the key expansion portion.

The Blowfish was invented to be speedy and safe. It may be modified to satisfy multiple security procedures because of its flexible key length. Generally, selecting a symmetric key encryption technique depends on the system in question's unique security needs and performance requirements. Blowfish strikes a decent mix between security and speed, whereas AES is typically regarded as the most secure solution. For older systems that are difficult to update to implement newer encryption algorithms, 3DES might be a practical option.

2.3.5 Public Key Cryptography

Two keys are employed within a public key cryptosystem, one for encrypting and the other for decrypting [28]. Whilst doing inverse operations, the two keys are logically linked. There can't be an easy way to get the decryption key from the enciphering key. Thus, anyone can encrypt communications, but only the intended receiver can decode them. The enciphering key can then be made public without jeopardizing the deciphering key. Arguably, a robust mathematical safe with a unique resettable combination lock with two combinations—one for locking and another for unlocking—is an image of a public key cryptosystem [41]. Anyone can lock up information since the locking combination is made available to the public. The information can only be accessed and retrieved by the intended recipient, who is aware of the unlocking combination.

Public key cryptography is considered very important to the security of transactions and the ownership of digital assets in cryptocurrencies. A decentralized database, a blockchain, is used by Bitcoin and other digital currencies to record and verify transactions. To encrypt and decrypt transactions, each user has a public key and a private key, which are fundamentally very long sequences of letters and numbers. While the private key is kept private and only utilized by the owner, the public key is made accessible to other users. A user launches a transaction using their secret key and broadcasts it to the network for verification when they want to transmit cryptocurrency to another user. The recipient's public key is included in the transaction, which is used to validate the legitimacy of the transaction and the ownership of the assets by the user who sent the payments.

2.3.6 RSA - Rivest-Shamir-Adleman

The cryptocurrency sector has taken on RSA encryption, one of the most frequently used public-key encryption algorithms in the world. Also, it is utilized to safeguard private keys in Bitcoin wallets. To prevent unwanted access to the wallet, private keys that are used to sign transactions must be given protection. These keys are encrypted using RSA encryption, making it more challenging for attackers to extract them. Apart from this, RSA is also the most used global technique which encrypts

data as it traverses over the Web to provide security and ensure the authenticity and secrecy of information [67]. The RSA methodology is very simple. RSA cryptosystem is one of the most prominent security algorithms, which comprises three phases i.e. Key formation, Encryption, and Decryption.
Key generation

- Choose two prime numbers, p and q, where p and q are not equal;
- Determine n=(p)(q);
- Determine (n) = (p -1) x (q-1);
- Choose an integer e such that gcd (n, e) = 1; e 1. (n);
- Determine the private key using d = -1 (mod n).
  The public key is PU = e, n. Private Key PR = d, n.

Encryption procedure:
Plaintext – Message “M” Ciphertext “C” = Me mod n
Decryption Procedure:
M = Cd mod n
Where ’M’ denotes Message, ‘p‘ and ‘q‘ are prime numbers, N is the modulus, ‘e‘ and ‘d‘ are public and private keys respectively.

RSA encryption scheme uses prime factorization. It leverages public key encryption, which allows anybody to use a public key to encrypt data before sending it over a network. To offer a private key to decrypt the information, it authenticates users and ensures network security. As a result, only authorized recipients can access the decrypted data. The RSA algorithm is applied for both digital certificates and data encryption. The key point is that factoring takes an excessively long for large integers. Although there may be an alternative, less difficult way, it remains to be proven that defeating the RSA algorithm is equal to factoring massive numbers [9]. By principles, large primes must be supplied for RSA. These can be produced by choosing random (odd) integers of the necessary size and determining if they are prime. If it transpires that the integer is a composite, a new candidate is chosen at random. This strategy must fulfil two conditions to be effective: 1) Tests for primality (Solovay-Strassen primality test and Miller-Rabin primality test) must be practical, and 2) there must be a reasonable likelihood that a randomly chosen odd integer is a prime.

2.3.7 DSA - Digital Signature Algorithm

Digital signatures are used to validate and authenticate documents and data. This is necessary to prevent tampering, digital manipulation, or forgery during the transmission of official documents. The discrete logarithm problem (DLP), a mathematical puzzle that has been considered to be tough to solve, provides the foundation for DSA. The approach employs a public key for message signing and a private key for verifying a signature. The algorithm’s security depends on how challenging it is to calculate the private key from the public key.

A set of domain settings, a personal key, a per-message secret number, a hash function, and the data that must be signed are utilized to compute a DSA digital signature. In the same domain settings, a public key that is mathematically linked to the private key used for creating a digital signature, the data is validated, and the same hash function as during the creation of the signature is employed to confirm a digital signature [46]. Key creation, signature generation, signature verification, and key exchange are the four processes that make up the DSA algorithm. During key generation, a user creates a public key and associated private key. Using their private key, the user computes a digital signature to sign a message, and the recipient uses the sender's public key to validate the signature. DSA can be used for key exchange, which entails securely exchanging keys between two parties, in addition to signing and verifying communications.

2.3.8 Cryptanalysis

The study and practice of deciphering codes, ciphertext, and encrypted text without the use of the actual key is known as cryptanalysis. It is the antithesis of cryptography, which is the study and development of algorithms and encryption cyphers. To crack encryption algorithms, cryptanalysts deploy a range of methods such as **Known-plaintext attack**: When the cryptanalyst has access to both the ciphertext and the corresponding plaintext. **Chosen-plaintext attack**: The cryptanalyst is able to choose the ciphertext that is decrypted. **Brute-force attack**: Cryptanalyst simply tries every possible key until they find the correct one. A survey study [47] offers an in-depth analysis of multiple cryptanalytic attacks on cyphers as well as defence strategies against the attacks. The impact of comprehending these assaults and corresponding defence for creating novel, secure cyphers or enhancing the security of already-existing ones. It classifies attacks according to the attacker's informational resources, memory needs, and processing time requirements. The overview covers many kinds of attacks on symmetric and asymmetric cyphers, such as side-channel, differential, and linear cryptanalysis, as well as brute-force assaults. Each attack type is thoroughly discerned, along with preventative steps that can be taken. It highlights how crucial it is to implement countermeasures while designing a cypher to make sure that it is impervious to these kinds of attacks. Common attacks against symmetric cyphers include Man-in-the-Middle, Boomerang, and Differential Cryptanalysis. Attacks on the discrete logarithm and integer factorization problems—which are used in the Diffie-Hellman key exchange and RSA encryption, respectively—are two frequent targets for asymmetric cyphers.

COPACOBANA is a low-cost, powerful cluster made up of 120 FPGAs that are specifically designed to break codes [[39]. It is a reconfigurable parallel FPGA machine with low communication and memory needs, making it ideal for computing tasks that may be parallelized onto separate nodes. Depending on the specific algorithm, COPACOBANA can perform several orders of magnitude better than off-the-shelf machines. The authors addressed a variety of cryptanalytical approaches that make use of COPACOBANA's processing capacity. These include time-memory trade-off tactics, which can be used to attack the well-known A5/1 algorithm used in GSM voice encryption, exhaustive key search attacks on symmetric cyphers, and an attack on a security feature used in the electronic passport (e-passport). Furthermore, effective ways to carry out increasingly intricate cryptanalysis on asymmetric cryptosystems have been presented, like number co-factorization for RSA and Elliptic Curve Cryptosystems (ECCs). Although COPACOBANA lacks dedicated memory modules, each FPGA has a finite amount of RAM blocks that can be employed to collect information for expanding attacks with realistic security criteria, such as attack duration and cost.

2.3.9 Cryptanalysis in cryptocurrencies

Side-channel attacks represent one of the most prevalent applications of cryptanalysis in cryptocurrency. These attacks exploit information inadvertently disclosed by cryptographic systems during their operation, such as timing details, power usage, or electromagnetic emissions [47]. Utilizing this data, it becomes possible to retrieve the secret key of the cryptographic system. In a brute-force attack, each potential key is systematically tested until the correct one is identified. Although brute-force assaults are time-consuming, they prove effective against encryption schemes lacking robustness [78]. Cryptocurrency developers continually strive to employ enhanced encryption techniques and establish security measures to thwart side-channel attacks, thereby enhancing the security of their systems. Simultaneously, cryptanalysts persistently devise innovative methods to crack encryption systems, engaging in an ongoing race against each other.

3 BlockChain Technologies

Blockchain technology enables decentralised transactions by creating an unchangeable ledger. It was first put forth in 2008 and put into practice for the Bitcoin cryptocurrency in 2009 [63]. The most widespread use of blockchains is in cryptocurrency systems like Bitcoin, where they are essential for keeping a safe, decentralised record of transactions. The four main features of blockchain technology are auditability, persistency, anonymity, and decentralisation. Blockchain design, common consensus methods used in blockchain, recent technological advancements and obstacles, and potential blockchain trends in the future. Applications built on blockchain technology are emerging, and in-depth studies of these applications are slated for the future [83]. Blockchain can be employed in several different kinds of financial services, including digital assets, remittance, and online payment because it enables payment to be completed without the use of a bank or other middleman. Furthermore, it can be utilised in other domains such as public services, smart contracts, the Internet of Things (IoT), reputation systems, and security services.

3.1 Architecture of Blockchain

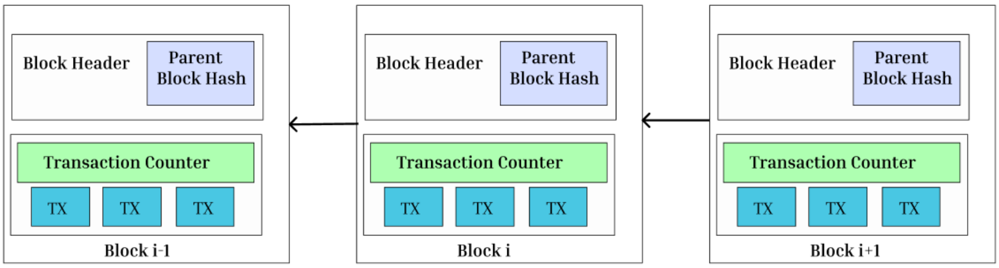


Figure 5: An example of blockchain which consists of a continuous sequence of blocks [83]

Comparable to a traditional public ledger, a blockchain is a series of blocks containing a complete list of transaction records. Figure 5 shows an illustration of a blockchain. A block has just one parent block since the block header contains the preceding block hash. It is vital to remember that hashes of uncle blocks—children of the block's ancestors—would likewise be kept on the blockchain [18]. A blockchain's genesis block, which is the first block without a parent block, is known as such. Next, I go into detail of blockchain's internal workings.

Block: As seen in Figure 6, a block comprises the block header and the block content. Specifically, the block header consists of:

1. Block version specifies which set of block verification guidelines to use;
2. The hash value of every transaction in the block is the Merkle tree root hash;
3. Timestamp: the moment expressed in universal time in seconds;

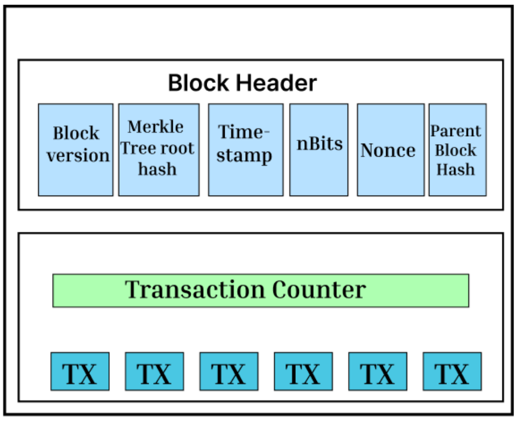


Figure 6: Block structure [83]

4. nBits: the desirable threshold for a block hash that is valid;
5. Nonce: a 4-byte field that typically starts at 0. It rises with each hash computation;
6. Parent block hash: a hash value of 256 bits pointing to the block before it.

Transactions and a transaction counter make up the block body. The block size and the size of each transaction determine the maximum number of transactions that can be contained in a block. Blockchain ensures the authenticity of transactions via an asymmetric cryptography approach [83].

Digital Signature: As I have discussed DSA in the second chapter every user possesses a set of both private and public keys. The transactions are signed using the private key, which will be kept secret. The network broadcasts the digitally signed transactions. There are two stages to a typical digital signature: the signing phase and the verification phase. For example, Alice, one user, wants to message Bob, another user. (1) During the signing stage, Alice uses her private key to encrypt her data, sending Bob both the original data and the encrypted result. (2) Bob uses Alice's public key to verify the value during the verification stage. Bob could then quickly determine whether the data has been altered or not. The elliptic curve digital signature method (ECDSA) is the standard digital signature algorithm used in blockchain.

Key Characteristics:

1. Decentralization: Unlike the centralised form (e.g., Bank), blockchain eliminates the necessity for a third party. In distributed networks, consensus techniques in blockchain are employed to preserve data consistency.
2. Persistency: Quick transaction validation is possible, and true miners would never accept a transaction that was invalid. Upon inclusion in the blockchain,

transactions are nearly impossible to remove or reverse. It may be possible to identify invalid transaction-containing blocks right away.

3. Anonymity: Every user has a created address that they can use to communicate with the blockchain; this address conceals their true identity [83].

3.2 Blockchain applications

In recent times, blockchain technologies have gained attention in both scientific and industrial spheres. This is because of their ability to solve several problems in various industrial domains. Examples include problems with safely exchanging transactional data, setting up effective supply chain procedures, and strengthening transparency. Blockchain technology, which uses distributed, shared, secure, and permission transactional ledgers, provides a practical solution to these problems. Many industrial applications are made possible using blockchain technology and their adaptability to various contexts. These applications benefit from better efficiency and security, improved traceability and transparency, and lower costs. Blockchain technology ensures the legitimacy of the performed agreements by combining the virtues of cryptographic algorithms and peer-to-peer networks. Without engaging the other participating entities, none of the parties involved may alter the approved and registered activity. This capability is ideal for performing various business agreements between a collection of geographically dispersed companies. Additionally, blockchain can guarantee the accuracy of recorded transactions over time and maintain the chronological order of occurrences. It is practically hard to falsify records or withdraw from an agreement since no one can unilaterally change any of the transactions that are recorded. Because of this, a wide range of companies and industries are thinking about using blockchain technology, and further study is underway to determine how best to do so [10].

IBM is a firm supporter of blockchain technology and its applicability in the broader commercial and industrial circle, evidenced by their significant investments in the technology and ongoing development of new features and functions [66]. With the launch of cryptocurrencies and their widespread use, blockchain emerged as a promising technology [34]. It is, nevertheless, beginning to emerge as a promising technology with a wide range of applications. The following subsections are expanded with several blockchain-based industrial applications that have numerous advantages for businesses and the industry. Following are a few of the many applications explored which are categorized by their domains.

3.2.1 Financial Applications

Inspired by its potential to successfully support cryptocurrencies, the financial industry naturally followed suit with blockchain applications in other financial domains. Generally, financial transactions between individuals and organisations are carried out through reliable third parties. These outside parties carry out four tasks [54]:

1. Verifying the authenticity of transactions;
2. Avoid duplications of financial transactions;

3. Signing up for and confirming financial transactions;
4. Acting as representatives for customers or partners.

Two of these functions—preventing duplicate transactions and recording and confirming financial activities—can usually be replaced by blockchain. Blockchain makes it simple to stop clients from making numerous payments totalling more than they owe, for example. Using regular checks, it is possible to carry out this act unlawfully. Nevertheless, this is not feasible with blockchain since every financial transaction needs to be validated jointly before it can be completed. Blockchain can also serve as a safe record of financial transactions that are made. After being added to the chain, no party engaged may alter this registration. Through group checks and verifications, it can also be utilised to validate the transactions that were carried out. Plenty of financial applications, like the ones that follow, are made possible by these two properties [10].

1. Digital Currencies: Digital currencies (aka Cryptocurrencies) are mainly based on blockchain technology. This will be discussed in more detail in Chapter 4. However, blockchain is used to perform, register, and verify payments using digital currency as well as to record and validate ownership of digital currency.

2. Stock Trading: The standard way of trading stocks is through a centralised authority, such as an exchange market, which records all trades and payments. However, there are typically additional expenses and settlement delays connected with this process. To resolve these problems, tZERO [5] created a blockchain-based platform that speeds up settlement and minimises costs while enhancing visibility and transparency. Cryptographically protected distributed ledgers are integrated into this platform to facilitate settlement operations.

3. Insurance Marketplace: Blockchain technology can facilitate transactions between various clients, policyholders, and insurance companies in the insurance business. Blockchain can be used for reinsurance transactions between insurance companies as well as for policy negotiations, purchases, and registration. It can also be utilised for claim submission and processing. Smart contracts can be used to automate many insurance policies, which can drastically lower administrative expenses [20]. Processing insurance claims, for instance, comes at a considerable administrative cost. Due to misunderstandings and conflicts, claims administration can frequently involve extremely complicated procedures. These issues can be avoided using smart contracts by arranging insurance contracts in more exact “if-then‘’ scenarios. This makes it possible to automate the terms’ implementation through digital protocols that precisely carry out the agreed-upon insurance policies, minimising effort and execution costs. Insurance companies can use this decrease to lower the price of their insurance products and increase their competitiveness in an effort to draw in more clients. Insurance companies can also introduce new automated insurance solutions for their clients without having to worry as much about the expenses and overhead of their administration. Moreover, blockchain facilitates the global expansion of insurance businesses.

4. Financial Settlements: Businesses and organisations can record, validate, and handle financial transactions using blockchain technology. It makes clearing procedures possible, which entails modifying financial obligations to permit payments. Financial settlement procedures in other blockchain-based applications, such as stock trading or logistics, can be enabled by integrating blockchain-based financial settlement systems with other blockchain-based applications [10].

3.2.2 Healthcare Applications

Patient data is one of the most delicate and important aspects of healthcare. The medical records of patients are typically dispersed throughout several systems that are run and owned by one or more healthcare organisations. The advancement of digital technology has made it possible to digitise patient data into what is often known as an electronic medical record (EMR). A number of concerns, including security and privacy, make it difficult for various healthcare providers and organisations to share electronic medical records (EMRs). Blockchain technology can facilitate safe electronic medical records and other forms of multi-provider sharing of patient data. A startup business named Gem created a blockchain-based network for creating universal healthcare data-sharing infrastructure and applications [69]. Additionally, Tirion, a different startup, created a platform for storing medical data. Also, this platform facilitates the audit and validation of medical records and procedures.

The healthcare industry can benefit from general cryptography theories that ensure information security but with far more subtle and granular concerns. Firstly, the network does not have to be as decentralized as public blockchains, which make all data available to everyone with an Internet connection [81]. Instead, a group of companies or organizations operating in the same industry and bound by comparable regulations may create a permission, small-scale blockchain that would be adequate to address the need for a central authority. On the other hand, it might adhere to the same codes as a conventional, stand-alone healthcare centre and successfully serve the healthcare community. In this case, smart contracts can also be used to extend the capabilities of blockchains similar to bitcoin, which can now support only pure cryptocurrency transactional data. They can also be used to implement more sophisticated logic that controls complex data and data structures and ensures that those transactions cannot be reversed. When this same scenario of data integration is used between popular edge device and app providers and certified and regulated medical entities as previously described, any historical record of data exchange would remain in the blockchain, allowing the network to see which sources typically offer reliable data and which ones might be rogue players in the ecosystem [80].

An authorized blockchain, in which only approved entities or organizations can participate in crucial decisions like adding or removing members and validating transactions to include them in the shared ledger, can be created via smart contracts that enforce a membership-based ecosystem [19]. Because users of a permissioned blockchain, including healthcare providers and experts, can exchange data utilizing the blockchain architecture, this model does not automatically establish a closed environment [82]. In other words, its maintainers are the only people with authority to access this blockchain architecture.

Next I will list some of the examples of the difficulties the healthcare sector faces including the solution offered by Blockchain, which may affect patient care, data management, and long-term financial viability:

- Interoperability: Healthcare data is frequently compartmentalized between several organizations and systems, making smooth data sharing and exchange challenging [81]. Blockchain can improve interoperability and data sharing by enabling the smooth transfer of healthcare data between various systems and organizations.
- Security and Privacy: Patient privacy and confidentiality may be jeopardized by cyberattacks and data compromises, which affect sensitive and private healthcare data. Blockchain technology can offer a safe, unhackable method for exchanging and storing private medical information, protecting patient confidentiality [80].
- Provider Identity Management: Keeping track of licenses, credentials, and provider identities can be difficult and time-consuming, resulting in administrative burdens and inaccurate provider data. By establishing a decentralized database with blockchain technology, provider identities, credentials, and licenses may be managed with less administrative work, and authenticity is guaranteed.
- Clinical Research: Information from clinical research is frequently dispersed and challenging to exchange, especially in studies of uncommon diseases where cross-regional data exchange is essential. Blockchain technology can facilitate the safe and transparent exchange of clinical research data, which is especially useful for studies on rare diseases where cross-regional data sharing is essential [81].
- Data Auditing and Fraud Prevention: Financial losses and higher healthcare expenses for patients and payers are caused by healthcare and insurance scams, which is a serious issue [80]. Blockchain's audit trail can assist in decreasing financial losses from deception, identifying and preventing fraud in the healthcare and insurance industries, and giving transparency in data exchanges.

3.2.3 Logistic Management Applications:

Applications for logistics management are software programs that assist in organising the transportation of goods, services, and raw materials from producers/sellers to consumer destinations. These may operate across several organisations and entities or as a component of a single organisation. Blockchain technology can offer strong support to make these applications possible. Multiple organisations participating in the operations is one of the challenges of logistics management. This could also involve several coordinated sub-activities carried out by several businesses, including manufacturers, storage facilities, transportation firms, and regularity authorities

[16]. Any logistics management programme should include a collection of features that allow users to plan, schedule, coordinate, monitor, and verify the tasks that are completed.

These kinds of operations can be effectively and safely supported by blockchain. Reducing time delays, management expenses, and human errors will be made possible by using the shared distributed ledgers in blockchain for the verification, archiving, and auditing of logistical transactions. Furthermore, using advanced contracts will speed up and reduce the cost of creating legally binding agreements by facilitating agreements between the participating companies. Numerous startups in this field are providing blockchain-based systems and applications for logistics management. *Provenance* (provenance.io) is one example; it offers a traceability system that connects suppliers and customers for various logistics tasks. *Hijro* (hijro.com), which provides an application platform to enable global supply chain management, is another example. However, there are several non-financial uses, including decentralised governance, online voting, and token systems for smart property ownership and incentives [12] [68]. Thus, beyond cryptocurrencies, some real-world uses for blockchain technology include strengthening cybersecurity, facilitating safe and transparent voting processes, and optimising supply chain management.

3.2.4 Food Product Traceability in Walmart

Regarding food traceability, it is essential to document the product's origin and its previous locations. It all started at Walmart in 2016 when the company's vice president of food safety gave his staff the task of tracking down the origin of a bag of sliced mangoes. His crew needed six days, eighteen hours, and twenty-six minutes. Even though all the data was already in the system, it took a while to get the details. Walmart then started to use a blockchain framework known as the Hyperledger Fabric [17] blockchain-based food traceability system which determines the provenance of the food product in seconds. Walmart currently tracks more than 25 items from five distinct vendors through the blockchain technology brought by IBM. Beyond following the path of the goods, the corporation may begin tracking other data, such as sustainability [7] .

Hyperledger Fabric is an open-source collaborative project aimed at advancing blockchain technology. It is not a firm, nor is it a cryptocurrency or blockchain. Instead, it is a ledger (chain code), smart contract, and system support for transaction management. However, it is permissioned and private [17]. Every member of the Hyperledger fabric must use a legitimate membership service provider to log in. Some components that make up fabric are orders, committers, endorsers, smart contracts, and validators. Its goal is to assist businesses in growing their blockchain network to process over a thousand transactions per second, enabling multiple enterprises to participate in BC. Additionally, the fabric contains fewer nodes than a public blockchain to boost processing speed for large amounts of data. Although it lacks a native currency, users can define assets on the client side. Users can engage in both private and public interactions with Fabric's permission [19].

3.3 Performance and Scalability

The three main aspects of blockchain scalability bottleneck are performance inefficiency, high confirmation delay, and function extension [79]. In China, “Tmal‘’, the most well-known online retailer, transaction volume of “Tmall‘’ surpassed 38 billion dollars on November 11 2019, with a peak order creation rate of 544,000 transactions per second (TPS). However, drawing a comparison of the above TPS with the data in Table 1 showing mainstream blockchain transactions TPS currently.

Table 1: TPS of mainstream Blockchain [3] [57]

Blockchain	TPS
Visa	17000
Mastercard	193
Bitcoin	7
Ethereum	27
Solana	50000
Avalanche	4500
Algorand	9
Polygon	7000
Polkadot	0.6
Tezos	40

Preferring their choice of design, Bitcoin and Ethereum have the lowest TPS of all the blockchains on the list. Ethereum is intended to be a platform for decentralised apps, while Bitcoin is intended to be a safe place to keep currency. These two blockchains place more emphasis on security than on speed. The transaction procedure has experienced a significant confirmation delay. The confirmation time is at least 10 minutes due to the 10-minute Bitcoin block production speed, and due to the splitting phenomena, it is typical to consider the transaction confirmed after 60 minutes. The validation process takes 15 seconds on even the best Ethereum [79]. Table 2 shows the current latency, scalability, and cost of mainstream blockchains.

The most crucial scaling performance metric for blockchains is transaction throughput, which demonstrates the network’s processing capacity. TPS is a popu-

Table 2: Latency of mainstream blockchain [2]

Blockchain	**Latency**	**Scalability**
Visa	0.5 Seconds	Very high
Mastercard	0.5 seconds	Very high
Bitcoin	10 minutes	Low
Ethereum	15 seconds	Low
Solana	0.25 seconds	Very high
Avalanche	0.5 seconds	Very high
Algorand	2 seconds	Very high
Polkadot	15 seconds	Medium
Tezos	30 seconds	Low

lar metric used to assess the performance or scalability of blockchain applications. Blockchain transaction throughput is dependent upon block size and block arrival time [72]. The more transactions that are added to a block, the faster a blockchain can process transactions. However, most blockchain networks have a fixed block size for security concerns. For instance, a Bitcoin block is one megabyte in size. Raising the block size could boost throughput but could also cause a security issue and lengthen the propagation time. Large blocks could make the network vulnerable to DDoS attacks. For this reason, the best trade-off block size must be found in order to protect network security. Sending blocks with greater frequency could boost a blockchain's throughput. A lower block-arrival time will allow for a higher TPS. There is a trade-off with the network's security, though. A fork is more likely to occur if blocks are processed so often since it will be challenging to synchronise the nodes due to their disparate processing capacities. The likelihood of double spending and other assaults will rise as there are more forks. Therefore, it is necessary to determine the best trade-off between the network's security and the block arrival time. Since every scenario has a different set of users and requirements, it is hard to ask for a blockchain system that can support every application. Therefore, to truly understand the importance of interconnection, we must implement the interaction between the chains, preventing blocks from becoming isolated from one another [79].

4 Cryptocurrencies

To stop fraud, all currencies require a mechanism to manage supply and impose different security features. Organisations such as central banks regulate the money supply and imbue physical currency with anti-counterfeiting characteristics in fiat currencies. Although these security measures make it more difficult for an attacker to steal money, they do not make it impossible. In the end, law enforcement is required to prevent people from disobeying the system's regulations [64]. Cryptocurrencies are digital or virtual money that run on decentralised networks powered by blockchain technology and employ encryption for security. Cryptocurrencies, as opposed to conventional currencies that are controlled and issued by financial organisations and governments, use cryptographic techniques to safeguard transactions, manage the generation of new units, and confirm the transfer of assets. The most well-known cryptocurrency is called Bitcoin, which was first offered in 2009 under the pseudonym Satoshi Nakamoto by an unidentified individual or organisation[63]. Since then, a large number of alternative cryptocurrencies—also known as altcoins—have been created, each with distinct features and uses. Decentralisation is the fundamental idea behind cryptocurrencies [40]. Conventional financial systems handle and verify transactions through centralised entities such as governments or banks. On the other hand, cryptocurrencies make use of a blockchain, a decentralised ledger. By recording every transaction across a network of computers or nodes, this distributed and irreversible ledger does away with the need for a central authority. Blocks are created from the grouping of transactions, and a chain is created by connecting each block to the one before it using cryptographic hashes. Security, immutability, and resistance to censorship are guaranteed by this transparent, decentralised architecture.

The decentralised nature of cryptocurrencies presents an additional challenge, as does their volatility. They are a perilous investment because of their price volatility. Because companies cannot predict how much cryptocurrencies will be worth in the future, it is challenging for businesses to accept them as payment. Ultimately there's the security concern tied up. Digital wallets, where cryptocurrencies are kept, are vulnerable to hackers. A person may lose all of their money if their wallet is compromised. This is a major worry for anyone considering making a cryptocurrency investment [53]. Although cryptocurrencies present some serious hurdles, the potential rewards are too tremendous to pass up. The conventional banking system might be overthrown by cryptocurrencies, which would also lead to the creation of a more financial systems.

4.1 Cryptocurrency technologies

A variety of technologies are used to power cryptocurrencies, each playing a crucial role in their operation and security. The decentralized nature of blockchain technology eliminates the need for intermediaries like banks or governments to manage and control transactions. By employing mathematical techniques to encrypt and decrypt data, cryptography makes sure that only those with the proper authority may access and handle their money [32]. Because every network member has access to the same transaction history, this decentralisation promotes transparency and confidence. Data is converted into unintelligible cyphers by encryption algorithms, which are then reversed by decryption algorithms to restore the original data's readable form. Cryptography is employed in the context of cryptocurrencies to safeguard private keys, which are necessary for token access and expenditure. Like passwords, private keys enable users to authenticate the ownership of their money. Cryptocurrency is sent and received via public keys, which are generated from private keys.

4.1.1 Cryptographic hash functions

The hash functions generate fixed-size hash values (digests) from arbitrary input data. These algorithms are used in the context of cryptocurrencies to generate a distinct hash for every block on the blockchain. This hash encapsulates all the data in the block and acts as a digital fingerprint for it. The next block uses the hash as a major feature to connect the blocks together in a chain. A single block's data change would require recalculating the hash for that block and all blocks after it. This characteristic makes the blockchain resistant to fraud and tampering by ensuring its integrity and immutability [45].

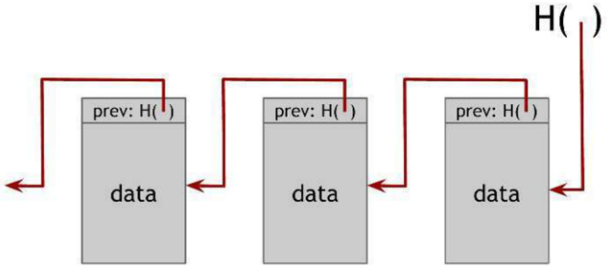


Figure 7: Block chain linked list that is built with hash pointers [64].

In Figure 7, a linked list is built using hash pointers. I will refer to this data structure as a blockchain, for example. In a blockchain, the preceding block pointer will be replaced with a hash pointer, as opposed to a standard linked list, where each block has data and a pointer to the block before it is in the list. Therefore, each block not only provides the location of the value from the preceding block but it also includes a digest of that value, enabling us to confirm that it hasn't changed. The top of the list is simply a standard hash-pointer pointing to the most current data block, which is what we keep. Making it immune to fraud and manipulation [64].

The Proof of Work (PoW) consensus process, widely used in cryptocurrencies such as Bitcoin, is based on cryptographic hash functions. In Proof of Work (PoW), miners strive to find a solution to a computationally challenging problem, with the network validating the solution [58]. To be included in the blockchain, a new block must satisfy certain requirements (difficulty level) in the hash function's output. Because hash functions are unexpected, miners have to invest a lot of processing power to discover a workable solution, which enhances network security and decentralisation [51] [36]. The hash functions are frequently used to generate cryptocurrency addresses, which are used for sending and receiving money. Hashing is used to create a shorter, fixed-length address using a user's public key. Since it is computationally impossible to reverse the hash function and retrieve the original public key, this procedure adds an extra degree of secrecy. Hashing functions also improve the network's overall security by strengthening the security of digital signatures used in bitcoin transactions [52]. Merkle trees, a hierarchical structure that effectively summarises the transactions within a block, are also built using cryptographic hash functions. The intermediate nodes are created by hashing pairs of child nodes, and each leaf node in the tree represents a transaction hash. The block header contains the Merkle root, which is the base of the Merkle tree and provides a succinct summary of all the transactions in the block. This makes it easier to efficiently verify if a transaction belongs in a block.

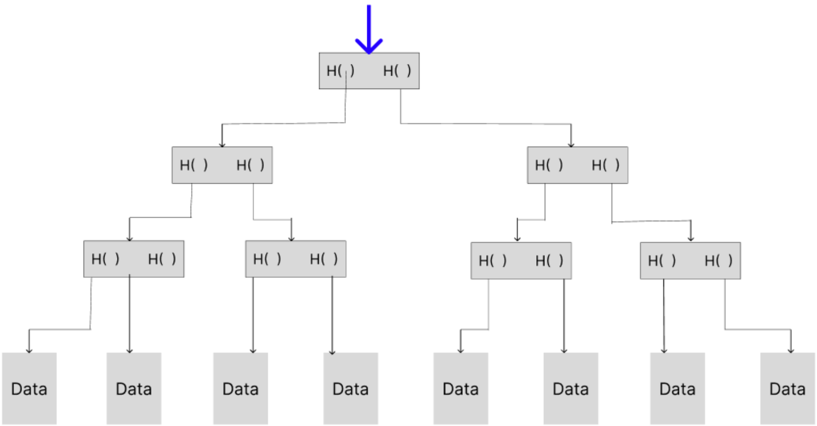


Figure 8: Data blocks are grouped in pairs, and the hash of each of these blocks are stored in a parent node. The parent nodes are in turn, grouped in pairs, and their hashes stored one level up the tree. This continues all the way up the tree until we reach the root node [64].

4.1.2 Digital Signatures

Together with hash functions, digital signatures, which were covered in Chapter 2, are the second cryptographic primitive that I'll need as building blocks for my discussion of cryptocurrencies. The idea behind a digital signature is to serve as the electronic equivalent of a handwritten signature on paper. Two characteristics of digital signatures that closely match the analogy of a handwritten signature are what we want. First of all, your signature is unique to you, but anybody who sees it can confirm its legitimacy. Secondly, we require the signature to be associated with a specific document in order to prevent it from being exploited to signify your approval or support of an unrelated document. This second feature is comparable to making sure that someone cannot take your handwritten signature, cut it off one document, and glue it to the bottom of another. Using the Elliptic Curve Digital Signature Algorithm (ECDSSA) instead of the standard elliptic curve “secp256k1,‘’ Bitcoin is said to offer 128 bits of security, meaning that breaking this algorithm is equivalent to performing 2^{128} symmetric-key cryptographic operations, like using a hash function [64]. Despite being a published standard, this curve is rarely used outside of Bitcoin; instead, the more widely used “secp256r1‘’ curve is usually utilised in other ECDSA-using applications (such as key exchange in TLS for secure web browsing). This is only a peculiarity of Bitcoin since it was decided upon by Satoshi [63] during the initial system specification and is now hard to alter.

4.2 Generation of Crypto Coins and Transfer Protocols

Let’s move on from cryptography and talk about the method that was employed to create cryptocurrencies. Based on my studying the book [64], I’ll progressively discover how the parts fit together and the real benefits of cryptographic operations like digital signatures and hash functions. I’ll talk about two extremely basic arbitrary cryptocurrencies in this section. Of course, explaining all the ramifications of Bitcoin’s operation will take up a significant portion of the remaining thesis.

4.2.1 JimmyCoin

Jimmy builds the phrase “generateCoin [newCoinID]‘’ and develops a unique coin ID (newCoinID) that he has never created before in order to generate a coin. Using his secret signing key, he then computes the digital signature of this string. The string is a coin when combined with Jimmy’s signature. Anybody can confirm that the currency is legitimate because it has Jimmy’s legitimate signature on a generation statement. JimmyyCoin’s second rule is that a coin’s owner may give it to another person. Cryptographic processes are used to transfer a coin; it is not as simple as emailing the coin data structure to the recipient.

Assume Jimmy would like to give Maria a coin he made. To accomplish this, he writes a new statement that reads, “Pay this to Maria‘’, where “this‘’ is a hash pointer to the relevant coin. Since identities are essentially simply public keys, Maria’s public key is denoted by “Maria‘’. Jimmy signs the string that signifies the phrase at the end. Jimmy must sign any transaction that uses the coin because he was the one who initially owned it. Maria becomes the currency owner when this data structure reflects his signed transaction. She may show the data structure with Jimmy’s legitimate signature. Thus she can demonstrate to anyone that she owns the coin. Moreover, it indicates a legitimate coin that belonged to Jimmy. Coin ownership and legitimacy are, therefore, obvious within the system. Maria can use the coin whichever she pleases once she has it. This is accomplished by her creating a statement that reads, “Pay this coin to Bob’s public key,‘’ where “this‘’ is a hash pointer to the coin she formerly had. Maria, of course, signs this document. Presenting this coin to someone can confirm that Bob is the rightful owner. They would confirm that the legitimate owner signed a document stating that they would “pay this coin to [new owner]‘’ at each stage by following the chain of hash references back to the coin’s inception.

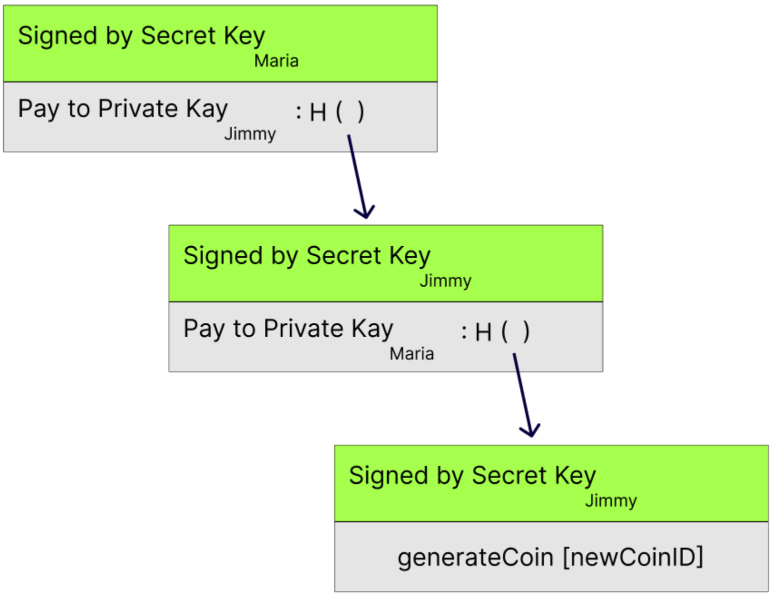


Figure 9: jimmyCoin. Shown here is a coin that’s been created (bottom) and spent twice (middle and top) [64].

To summarize, the rules of JimmyCoin are:

- Jimmy only needs to sign a declaration stating that he is creating new coins and provide a unique coin ID to do so;
- A coin can be transferred to another person by the owner signing a declaration that reads, “Pass on this coin to X” (where X is a public key);
- By following the chain of hash references back to Jimmy’s inception and confirming each signature along the way, anyone can confirm the legitimacy of a coin.

Naturally, there is a serious security issue with JimmyCoin. Assume that Maria sent Bob her signed declaration and transferred her coin, keeping everyone else in the dark. She may submit a second signed statement giving Charles the exact same amount of money. Charles perceives the transaction as entirely legitimate, and he now has ownership of the currency. Both Charles and Bob may legitimately argue that they are the rightful owners of this coin. Because Maria is spending the same coin twice, this is known as a double-spending attack. We instinctively know that coins aren’t meant to function that way. Actually, one of the main issues that any cryptocurrency must address is double-spending assaults. JimmyCoin is not safe since it cannot prevent the double-spending attack. JimmyCoin isn’t quite up to par as a cryptocurrency, despite its simplicity and striking resemblance to Bitcoin in terms of its coin transfer method.

4.2.2 PeterCoin

To address the issue of double-spending, I want to create a new cryptocurrency that I shall refer to as PeterCoin. Although PeterCoin is based on JimmyCoin, its data structures are slightly more complex. The primary concept is that Peter, a specified entity, publishes an append-only ledger that includes the complete history of all transactions. Any data written to this ledger will remain forever, thanks to the append-only attribute. We can utilise the ledger to prevent double-spending by mandating that all transactions be recorded in the ledger before acceptance, provided that it is really append-only. In this fashion, if coins were ever transported to a different owner, it would be made publicly known.

Peter can create a digitally signed blockchain, which is the data structure we previously mentioned, to accomplish this append-only capability. It's a sequence of data blocks, each containing a single transaction (in reality, we would actually optimize by grouping several transactions into a single block, just like Bitcoin does.) Every block contains a hash pointer to the previous block, the transaction's contents, and the transaction ID. The last hash reference, which connects all of the data in this structure, has been electronically signed by Peter, who then broadcasts the signature and the blockchain.

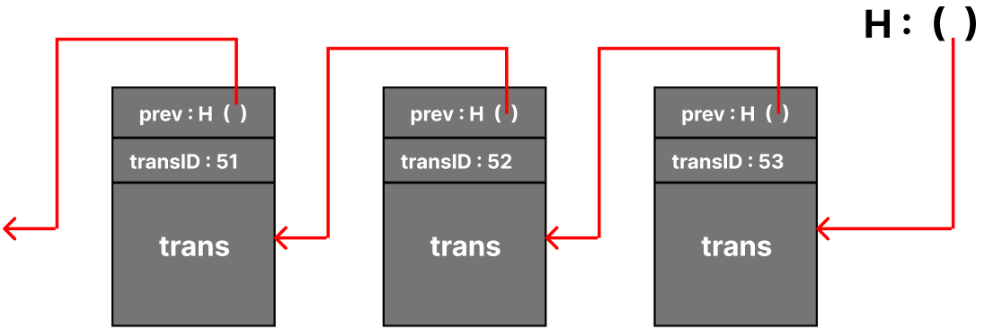
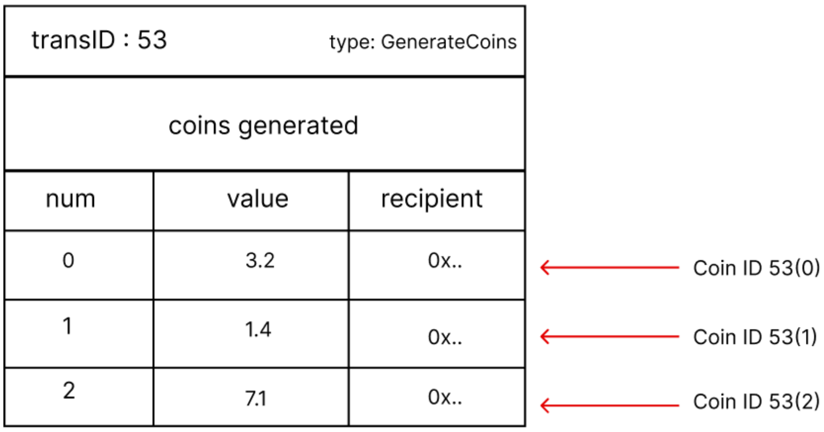


Figure 10: PeterCoin blockchain [64].

A transaction is only considered valid in the PeterCoin blockchain if it is signed by Peter. By looking for Peter's signature on the block where a transaction appears, anyone may confirm that Peter approved it. Peter ensures that he does not approve of a transaction that aims to double-spend a coin that has already been spent.

Why is having Peter sign each block not enough? Why do we also need a blockchain with hash pointers? This guarantees the append-only feature. Because of the hash references, if Peter tries to modify an existing transaction or add a new one to the history, it will impact all subsequent blocks. The change will be visible and simple to detect as long as someone monitors Peter's most recent hash pointer. If Peter had signed each block separately in the system, you would have to record each and every signature Peter ever provided. Any two people can easily confirm that they have seen the same history of transactions signed by Peter, thanks to a blockchain.

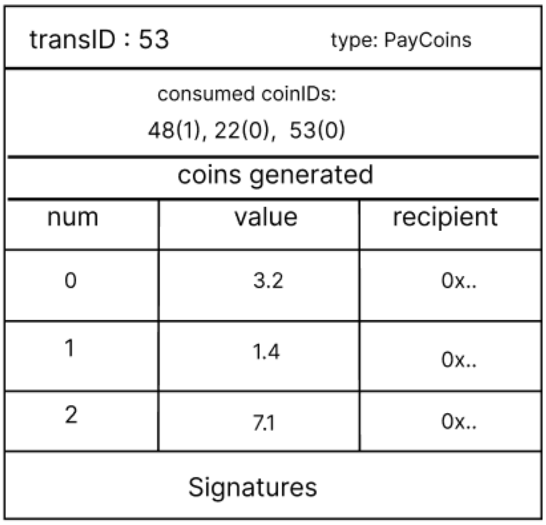


transID : 53		type: GenerateCoins
coins generated		
num	value	recipient
0	3.2	0x..
1	1.4	0x..
2	7.1	0x..

Figure 11: *GenerateCoin transaction*: Several coins are created by this GenerateCoins transaction. Within the transaction, a serial number is assigned to every coin. Every coin has a value as well; it is equivalent to a specific amount of PeterCoin. Last but not least, every coin has a recipient, which is a public key that receives the currency at creation. Thus, CreateCoins generates many new coins with various values and designates certain individuals as their original owners. By CoinIDs, we symbolise coins. A transaction ID and the coin's serial number within that transaction are combined to create a CoinID [64].

There are two different types of transactions in PeterCoin. The first type is GenerateCoins, which functions similarly to Jimmy's ability to create new coins in JimmyCoin. I'll somewhat expand the semantics with PeterCoin to enable the creation of numerous coins in a single transaction. If Peter signs a GenerateCoins transaction, it is absolutely legitimate by definition. Just like I didn't worry about JimmyCoin's selection process for the business authorised to create coins, I won't worry about when or how many coins Peter is authorised to make. PayCoins are the second type of transaction. It eliminates some coins by consuming them and produces new ones with the same total value. It's possible that different persons own the new coins (public keys). Each person paying with coins must sign this transaction. Therefore, in order to indicate that you are truly comfortable with spending this coin, you must digitally sign the transaction if you are the owner of one of the coins that will be used in it.
According to PeterCoin's rules, a PayCoins transaction is considered valid if four conditions are met:

- The coins that were eaten are legitimate, meaning they were actually created in earlier transactions;
- The consumed coins were not previously used in an earlier transaction. In other words, this isn't a double-spend;
- The entire value of the coins that were entered and the coins that are extracted from this transaction are equal. That is, Peter alone is capable of producing new value;
- All of the coin owners who have consumed their coins have duly signed the transaction.



transID : 53 type: PayCoins

consumed coinIDs:
48(1), 22(0), 53(0)

coins generated

num	value	recipient
0	3.2	0x..
1	1.4	0x..
2	7.1	0x..

Signatures

Figure 12: A PayCoins Transaction.

Peter will accept this PayCoins transaction as long as all of those requirements are satisfied. By adding it to the blockchain, he will make it part of history and make it visible to all users that this transaction has occurred. The participants can only acknowledge that the transaction has occurred at this stage. Even if it satisfies the first three requirements, it could be intercepted by a double-spending transaction until it is published.

This system's coins are unchangeable; they cannot be split, divided, or merged. Every coin is generated once during a single transaction and then used up in a subsequent transaction. However, we may use transactions to achieve the same result as being able to split or combine coins. To split a coin, for instance, Maria would begin a new transaction, consume the original coin, and then generate two new coins with the same total value. She may have those two new coins returned to her. Thus, despite the immutability of the currencies in this system, it retains all the flexibility of a system without immutable coins.

4.3 Consensus Mechanism

In the realm of managing the backend for a large social networking company like Facebook, the challenges of maintaining a distributed database with thousands or millions of servers necessitate a robust distributed consensus protocol. This protocol serves as the foundation for building massively distributed key-value stores with impacts that go beyond standard applications. These shops provide access to various uses, such as creating a public key directory or a distributed domain name system. A distributed consensus protocol is defined technically as one that maintains consensus across nodes even when there are imperfect or malevolent actors present [64].

What does this signify in relation to Bitcoin? Remember that Bitcoin is a peer-to-peer system that can help you comprehend how distributed consensus might function in the system [58]. In reality, Alice broadcasts a transaction to every Bitcoin node that makes up the peer-to-peer network when she decides to pay Bob. As an aside, you might have noted that Bob's machine is not shown in Figure 13 even though Alice broadcasts the transaction to every Bitcoin peer-to-peer node. Of course, it's feasible that Bob is in charge of one of the peer-to-peer network's nodes. In fact, it could be a good idea to start a node if he wishes to be notified that this transaction actually happened and that he was paid. That being said, Bob does not have to be watching the network; he can receive the money without running a node. Whether or not he runs a node on the network, he will have these bitcoins. What is it that the nodes in the Bitcoin network could wish to agree upon exactly? The nodes must concur on precisely which transactions were broadcast and the sequence in which they occurred because different users are broadcasting these transactions to the network. As a result, the system will have a single global ledger. Remember that PeterCoin groups transactions into blocks for optimisation. In the same way, the consensus is reached in Bitcoin block by block [64].

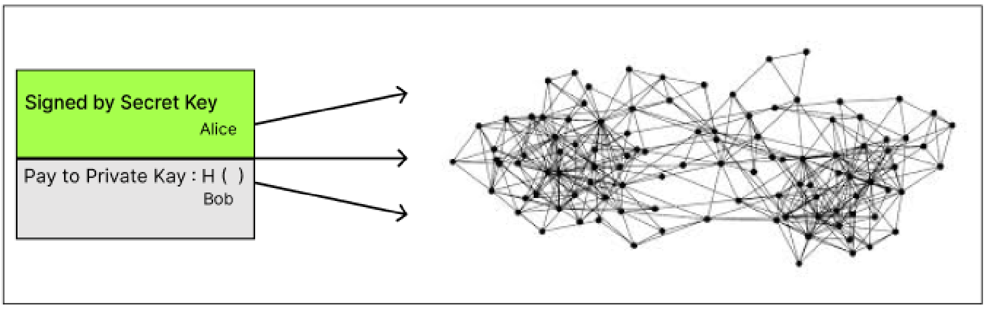


Figure 13: Broadcasting a transaction In order to pay Bob, Alice broadcasts the transaction to the entire Bitcoin peer-to-peer network.

Every node in the peer-to-peer network, therefore, has a ledger at any one time that comprises a series of blocks, each of which has a list of transactions that they have all agreed upon. A pool of ongoing transactions that each node is aware of but has not yet been added to the blockchain is also available to it [43]. Since agreement has not yet been reached for these transactions, every node may, by definition, have a slightly different copy of the outstanding transaction pool. In reality, this happens because there are imperfections in the peer-to-peer network, which means that certain nodes may have learned about a transaction that others are unaware of.

In precise terms, how do nodes reach a consensus on a block? One method to achieve this is to have each node in the system suggest its own outstanding transaction pool to be the next block at regular intervals, say every 10 minutes [50]. The nodes then carry out a consensus protocol, with the input of each node being a proposed block. Even though some nodes might be dishonest and include bogus transactions in their blocks, we might trust that most other nodes are sincere. The output will be a valid block chosen if the consensus mechanism is successful [83]. As long as the block is genuine, the output is still valid even if it was presented by just one node. It's possible that some legitimate outstanding transactions were missed by the block, but this is not an issue. A transaction might simply wait to be included in the following block if it somehow missed this one [43].
Before delving into the details of Bitcoin, let me first tell how the consensus algorithm works in it [64]:

1. Every node receives a broadcast of new transactions;
2. New transactions are gathered by every node into a block;
3. A random node broadcasts its block during each round;
4. Only after all transactions within the block are legitimate (unspent, valid signatures) will other nodes accept the block;
5. Nodes incorporate the block's hash into the subsequent block they generate as a means of indicating that they accept it.

4.4 Bitcoin Blocks and Network

Every transaction is created and redeemed separately. However, as discussed earlier, transactions are arranged into blocks. The rate at which new transactions may be approved by the system would be substantially reduced if miners had to reach an agreement on each transaction separately. Because many transactions can be included in a single block, a hash chain of blocks is also far shorter than a hash chain of transactions [13]. This will greatly increase the efficiency of the blockchain data structure verification process. A brilliant fusion of two distinct hash-based data structures creates the blockchain [83]. A hash chain of blocks is the first. A hash pointer to some transaction data, a block header, and a hash pointer to the block before it in the sequence are all included in each block. Every transaction included in a block is arranged in a per-block tree in the second data structure. We can efficiently obtain a digest of every transaction in the block thanks to this Merkle tree. The majority of the information contained in the header relates to the mining puzzle, which will be covered in the next sections. For a block to be considered genuine, its hash must begin with a significant number of zeros in the block header.

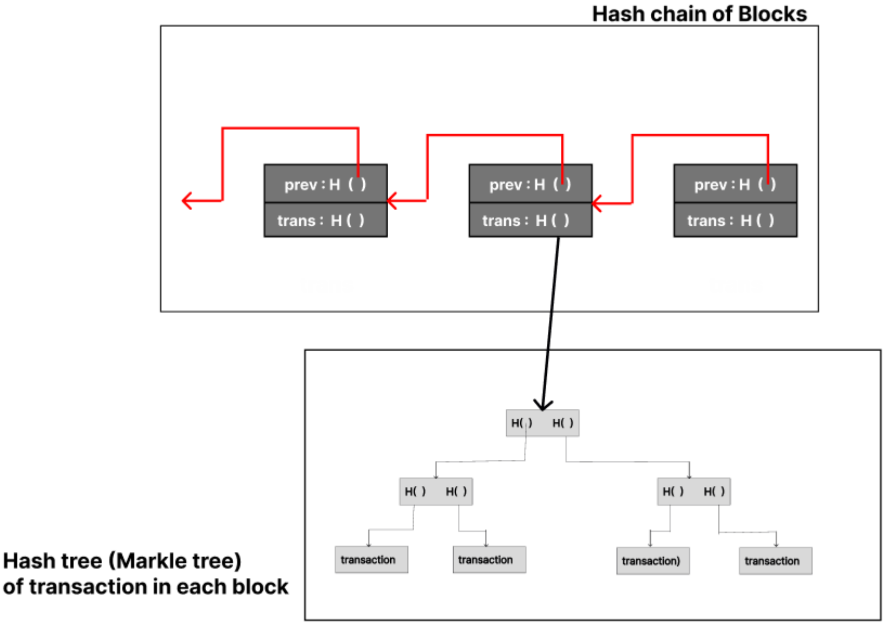


Figure 14: BTC chain contains two different hash structures [64].

The header also includes a time stamp, a variable “nonce‘’ that miners can modify, and “bits‘’, a measure of how challenging it was to locate this block. The only thing that is hashed during mining is the header [13]. Therefore, all it takes to validate a chain of blocks is a glance at the headers. The “mrkl root‘’ field, which represents the transaction tree’s root, is the sole transaction data that is contained in the header. The ideal approach is to investigate the blockchain yourself to gain a better understanding of the block format and transaction format. This data is available on a number of websites, including blockchain.info. We may search for transactions with complex scripts, examine the block structure to discover how blocks relate to one another, and view the graph of transactions to determine which transactions redeem which other transactions. Since the blockchain is a publicly accessible data structure, programmers have created attractive wrappers to allow for graphical exploration.

The Bitcoin network lacks a hierarchy and unique nodes, functioning as a peer-to-peer system. Any machine can join as a node with equal rights and capabilities using a random topology. Because the network is dynamic, nodes can come and go. Departures are handled politely by implicit forgetting, which occurs when a node is not used for a predetermined amount of time. To become a part of the network, a new node must establish communication with a seed node. This starts a random process that ends with complete membership [15]. Maintaining the blockchain is the core goal of the Bitcoin network, which is accomplished by using a straightforward flooding algorithm or gossip protocol to spread transactions. A transaction is broadcast to all connected nodes by the user and goes through several validation tests. Nodes use a race condition to prevent double-spending by holding transactions in a pool until they are uploaded to the blockchain. Because the network is decentralized, different logic may be implemented by different nodes, highlighting the necessity for each node to carry out its own checks. The Bitcoin network's design, which prioritizes simplicity and decentralization over a structured network, has issues with propagation time and efficiency [13]. Approximations indicate that the network has different sizes, is dynamic, and lacks a central authority for measurement. The complete blockchain is maintained by fully validating nodes whose storage needs are in the low tens of gigabytes. Furthermore, there are lightweight nodes that rely on fully validating nodes for transaction verification rather than storing the entire blockchain, which can result in significant cost savings. Much of the network now depends on the bitcoind library, which is kept up to date by developers at Bitcoin Core, even if more varied implementations are desired [64].

4.5 Bitcoin adoption and usage

The key to effectively storing and maintaining Bitcoin is protecting your secret keys. The three main objectives of crucial management are convenience, security, and availability. Finding a balance between these goals takes time and effort. Storing keys locally on a computer or smartphone is one straightforward approach that makes spending convenient and effortless. Nevertheless, there are issues with security and availability using this method. Coin access may be compromised if the gadget is misplaced, malfunctions, or corrupted. Keeping keys on a local device is like keeping cash in a wallet - referred to as "hot storage‘'; it's handy for small-scale transactions but not so safe for big-ticket items. Several trade-offs exist between convenience, security, and availability when using key management strategies. Although local storage is easy to utilize, it could be more reliable. Users can choose more secure options like cold storage or hardware wallets to protect more significant amounts. Finding the ideal balance relies on personal tastes and the amount of risk that users are ready to take when handling their cryptocurrency keys [64].

4.5.1 Wallets

When keeping bitcoins locally, usually a wallet software is used, a program that tracks all of your money, handles all the information related to your keys and makes everything easy to use with a good interface. If you want to send 6.50 Euros worth of bitcoins to your local coffee shop, the wallet software is handy because you typically want to use many different addresses with different associated keys. As I remember, creating a new public/private key pair is easy and we can utilize this to improve our anonymity or privacy. Wallet software gives a simple interface that tells you how much balance is there in your wallet. When we want to spend bitcoins, it handles the details of which keys to use, to generate new addresses, and so on [13].

The first form of Bitcoin wallet designed as a reference implementation was a desktop wallet. Many users use desktop wallets because of their capabilities, independence, and control. Operating on widely used operating systems like Windows and macOS presents specific security challenges, as these platforms are frequently unreliable and inadequately set up [61]. The most widely used type of Bitcoin wallet is a mobile wallet. These wallets, compatible with Android and Apple iOS smartphones, are frequently a fantastic option for first-time users. Although many are made to be straightforward, power users can also find fully functional mobile wallets. Most mobile wallets request information from remote servers to avoid downloading and storing significant amounts of data, which reduces your privacy by allowing third parties to learn about your Bitcoin addresses and quantities. Web wallets are accessible via a web browser and keep the user's wallet on a third-party server. Because it relies entirely dependent on a third-party server, this is comparable to webmail. While the user retains control over the Bitcoin keys thanks to client-side code that runs in their browser, some of these services jeopardize their privacy due to the user's reliance on the server [13]. But most demand control over users' Bitcoin keys in return for user-friendliness. Keeping significant sums of Bitcoin on unaffiliated computers is not encouraged. To obtain Bitcoins for the first time, one needs to find someone else who possesses them and purchase some directly from them. This is the most straightforward approach. Attending a local Bitcoin meetup listed on Meetup.com is one way to meet others with bitcoins.

- Sell goods or services for bitcoin to earn bitcoin. Sell your programming abilities if you are a programmer. Work as a hairstylist and earn bitcoins by cutting hair;
- Make use of the local Bitcoin ATM. An ATM that takes cash and deposits bitcoins into your smartphone wallet is known as a Bitcoin ATM (for example, a Bitcoin ATM in Skanssi shopping mall, Turku, Finland);
- Make use of a Bitcoin exchange connected to your bank account. Currently, currency exchanges in several nations provide a market for buyers and sellers to trade bitcoins for local money. Services that publish exchange rates, like BitcoinAverage, frequently display a list of Bitcoin exchanges for every currency.

4.5.2 Encoding Keys

We also need an approach to exchange addresses with the other party—the address to which bitcoins are sent—to send or receive bitcoins. Addresses to be transmitted from spender to recipient are encoded either as a text string or as a QR code [64]. We collect the bits of the key and change it from a binary number to a base 58 number to encode an address as a text string. Next, we encode each digit as a character using a set of 58 characters, known as base58 notation. Why is 58? That is the amount we obtain when we include all characters—upper and lower case, as well as digits—while excluding a few that could be unclear or appear to be different characters. For instance, the capital letters "O‘' and zero have been removed due to their striking similarity [40]. This makes it possible to read encoded addresses aloud over the phone or, if needed, to read them from printed paper and enter them in. Ideally, techniques like QR codes can be used to transmit addresses instead of laborious manual procedures.

The address that received the very first Bitcoin block reward in the genesis block, base58 encoded:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

The QR code, a primary type of two-dimensional barcode, is the second way to encode a Bitcoin address. One benefit of a QR code is that it may be instantly converted into a sequence of bits corresponding to the appropriate Bitcoin address by using Wallet 102 software and snapping a picture of the barcode with a smartphone. For instance, this can be helpful in a store where the checkout system may provide a QR code that you can scan with your phone to send money to that address. Additionally, it helps in phone-to-phone exchanges [13].

When appropriately used, Bitcoin offers consumers far more anonymity than traditional payment methods. This is one of its advantages. When you purchase, hold, and use Bitcoin, you are not required to give sensitive, personally identifying information to outside parties. However, national and international laws frequently apply if Bitcoin interacts with established systems, including currency exchanges [23]. We often must submit identification documentation and banking details to trade Bitcoin for our home currency. Users should be aware that connecting a Bitcoin address to a person's identification can make it easier to identify and follow other related transactions, including past ones. This is one of the key reasons why so many users keep separate exchange accounts from their wallets.

4.6 Transaction Fee

Every transaction added to the Bitcoin blockchain may be subject to a transaction fee. The difference between the total value of coins entering a transaction and the full value of coins exiting it is the precise meaning of a transaction fee. Because a standard transaction cannot produce cash, the inputs must always be at least as significant as the outputs. However, if the inputs are more important than the outputs, the difference is considered a transaction fee, which is paid to the miner who created the block containing this transaction [40]. I will confine my discussion to how transaction fees are set in Bitcoin as of early 2015; however, the economics of transaction fees are fascinating and intricate. Why are there transaction fees at all? The explanation is that relaying your transaction requires someone to pay a fee. The Bitcoin nodes must relay your transaction, and for a miner to compile it into a block, they must pay a small fee. For instance, if a miner finds a partnership that is marginally larger than the others because it includes your transaction, it will take a little longer to spread around the network. The likelihood of the block becoming orphaned increases if another miner finds a block nearly simultaneously. Therefore, adding your transaction has a cost to the miners as well as the peer-to-peer network. The purpose of a transaction fee is to cover the expenses miners spend to handle your transaction [42]. The current system does not pay nodes while operating a node is significantly less expensive than being a miner. In most cases, you have complete control over the transaction charge. There is no price to pay, or you could charge a hefty one. Generally speaking, it makes sense that your transaction will be relayed and recorded more promptly and reliably if you pay a higher transaction charge. Transaction fees as of right now by default. Currently, the majority of miners anticipate the following transaction fees [64]: First off, if a transaction satisfies all three of these requirements, there is no fee assessed:

1. The transaction is smaller than 1000 bytes;
2. Every output is greater than or equal to 0.01 BTC;
3. The priority is sufficiently high.

The formula for determining priority is (transaction size / (sum of input age * input value). Put differently, take a look at each input in the transaction, multiply its age by the value in bitcoins, and then add up all of those products. Remember that a transaction output matures faster the longer it remains unspent and increases in priority when it is. Your transaction will be relayed and recorded on the blockchain without incurring fees if all three conditions are met. If not, a fee is assessed, which, as of 2015, was only a tiny portion of a US penny per 1000 bytes (about 0001 BTC). A transaction typically consists of 148 bytes for each input, 34 bytes for each output, and 10 bytes for other data. Therefore, 400 bytes would be involved in a transaction with two inputs and two outputs. Currently, most miners implement the aforementioned fee structure, which implies that they will either serve incomplete transactions or fail to deliver the required transaction fees [23]. However, some miners disregard these regulations and will record and proceed with a transaction even if it only pays a minimal fee or none at all. If a transaction is incomplete, it will likely still be included in the blockchain. However, paying the standard fee will enable your transaction to be recorded more quickly and reliably. As a result, most wallet software and payment services incorporate the traditional fee structure into ongoing payments, so you will likely notice a small amount deducted for transaction fees when you conduct regular Bitcoin business [13].

4.7 Energy consumption and Mining

Even though blockchain is a reasonably secure platform, energy usage can rise significantly, mainly when mining has begun, which is a significant worry for the sector [30]. Validating the proof of work algorithm involves trial and error matching the hash value [38]. For instance, bitcoin miners need ten minutes on average to create a new block. It is highly encouraged to use this technology, where energy consumption is a significant concern for many entities to ensure data security and integrity [49]. According to statistics, a dramatic increase in the total number of cryptocurrencies from 2013 to 2022 was sighted. All of these virtual currencies aren't trading on the market, either. These cryptocurrencies are mined using various algorithms. Of all the digital currencies available, bitcoin is the most widely used and well-liked one worldwide. The mining of Bitcoin requires a significant amount of energy. According to a Business Insider article published in September 2021 by Eugene Kim, over 0.5 percent of all electricity consumed worldwide is used for Bitcoin mining, roughly seven times more energy than Google uses annually. The pace of the rise in electricity consumption has been noticeable each year, and in 2021, the consumption was about six times more than in 2017. However, over that same time frame, the amount of electricity used for Bitcoin mining grew steadily, ultimately raising the cost of mining Bitcoin [43].

The primary cause for the high energy consumption in Bitcoin mining is the proof-of-work technique used to solve a challenging mathematical problem [34]. Anybody can join the network and earn rewards by figuring out the mathematical puzzle on this open platform for the public. The Proof of Work (PoW) consensus technique is employed to both validate transactions and produce new blocks for the blockchain network. The distributed ledger in the blocks is used to compile all of the transactions sent by the blockchain network's participants after they have been validated [83]. All users in the network will be informed that, even though millions of people are competing to solve the challenge, only one person will be deemed the winner—the one who can solve the cryptographic puzzle the quickest. Therefore, in relation to the winner, the Bitcoin mining power consumption is not that great. However, the individuals who cannot answer the riddle cause their computers to consume a significant amount of energy in the process. Figure 15 depicts the Bitcoin mining process, in which all participants attempt to solve a challenging mathematical puzzle to determine which nonce can be matched with the desired value.

As a miner, the primary action you do is create a Merkle tree by gathering a set of valid transactions from your pending transaction pool [64]. You can, of course, decide how many transactions to include up to the block's maximum size. Next, you make a block with a header pointing to the block that came before it. There is a 32-bit nonce field in the block header. You experiment with different nonces until the block's hash falls below the target or roughly until the block has the necessary number of zeros. To find the nonce that certifies the block, a miner may start with a nonce of 0 and increase it by one at a time. Most of the time, you'll attempt every conceivable 32-bit nonce value, but none of them will result in a hash that is legitimate. You will now need to make more adjustments. The complete Merkle tree of transactions must update when the nonce parameter in a coinbase transaction is changed. Changing the additional nonce in a coinbase transaction is a far more expensive operation than changing the nonce in the block header since the change will propagate up the tree. Because of this, miners primarily focus on modifying the nonce in the block header and only switch to the coinbase nonce when they have tried every one of the 2^{32} nonces in the block header and still haven't found a working block [43]. A significant amount of processing power is needed to solve the mathematical puzzle, which depends on the following problems: i) Hash function, ii) Integer factorization, and iii) Guided Tour Puzzle protocol.

Hash function: When mining Bitcoin, chunks of data are sent in, and the value is reduced to a set format of 256 bits using the SHA-256 cryptographic hashing algorithm. The out-hash value fixes a 256-bit or 64-bit hexadecimal value, regardless of the input. There is no easy way to obtain the hash value because it requires a

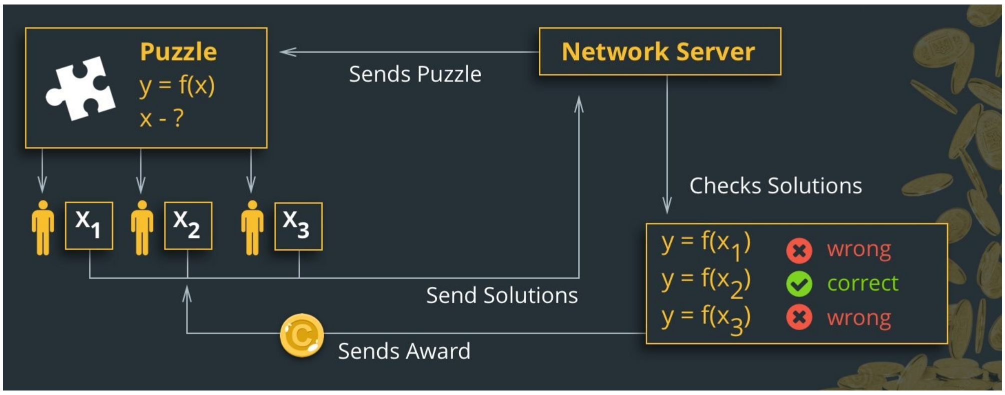


Figure 15: Bitcoin Mining Process [4].

great deal of computer power and numerous input data points that must be utilized on a trial basis.

Integer factorization: One way to safeguard the public key encryption procedure is by using integer factorial. This is how the multiplication of two other integers results in the current whole number [11].

Guided Tour Puzzle protocol: The Guided Tour Puzzle protocol guards against DoS attacks on the blockchain network[73]. Additionally, it insists on concentrating on the nodes in order to compute the memory-bound puzzle, assisting users in making use of idle processing capacity.
Around 2016 blocks or roughly every two weeks, the mining difficulty varies. It is modified using the formula:
next-difficulty = (previous-difficulty * 2016 * 10 minutes) / (time to mine last 2016 blocks)
which takes into account the miners' productivity during the preceding 2016 blocks.

Currently, the Bitcoin blockchain network is expanding more quickly, users are having more trouble solving cryptographic puzzles, and the algorithm requires more power to solve them, meaning that mining Bitcoin uses more electricity. In the past, mining Bitcoin simply required a CPU, which is extremely sluggish and uses a lot of energy. For the same aim, specialized gear known as GPU is utilised to reduce the cost of mining. A GPU can process data 100 times quicker than a CPU. Another alternative that is superior to GPU, CPU, and FPGA is Applications Specific Integrated Circuit (ASIC) [43].

4.7.1 Contrasting Fiat and Digital Money Printing

The nature of the two operations differs, therefore producing new cryptocurrency is not the same as printing money without restrictions. Let's examine how and why the process of creating new cryptocurrency differs from the ostensibly limitless process of generating fiat money.

Within a blockchain network, consensus processes usually control the issuance of new coins. For instance, in Proof of Work (PoW) systems, miners have to work out challenging mathematical puzzles to approve and append transactions to the blockchain. They can be rewarded with freshly made coins for their efforts. Validators in Proof of Stake (PoS) systems are selected to build new blocks according to the quantity of cryptocurrency they own and are prepared to "stake" as collateral. New cryptocurrency coins are frequently created and validated in a decentralised fashion, depending on the agreement of network users [22]. Over the entire process, no one entity has complete control. On the other hand, a central authority, such as a government or central bank, is typically in charge of creating and managing traditional fiat currencies. These authorities usually base their decision to issue more money on monetary policy and economic factors. The process is not decentralised, and regulatory limitations are in place to stop excessive printing.

The supply of specific cryptocurrencies, like Bitcoin, is limited. For example, the maximum number of coins in Bitcoin is 21 million . This scarcity is an essential feature of the cryptocurrency's creation and is incorporated into the protocol. The supply of conventional monetary currencies is only sometimes constant. Theoretically, central banks might print additional money, which could raise concerns about inflation and devaluation if they did so excessively [53].

4.8 Economic Impact of Cryptocurrencies

More than 1800 distinct cryptocurrency varieties were in use in 2018 [48]. As of August 13, 2020, there were 6442 cryptocurrencies in circulation, according to coinmarketcap.com [21]. While some of the new cryptocurrencies make it, others vanish within a few days. Each cryptocurrency has unique qualities that affect both its stability and cost, as well as the connections between them. Significant movements can be caused by a number of factors, including investor expectations and market uncertainty. From an economic perspective, there are several disagreements on the nature of Bitcoin and its intended uses. As a result, while some writers view Bitcoin as a means of trade, others view it as a riskier financial venture. The recognition of cryptocurrencies as a financial asset is where Corbet begins [22]. According to Frisby, Bitcoin appears to have the qualities of money and even performs better than fiat money [33]. It is, therefore, appealing due to its robustness, divisibility, portability, high liquidity, and reduced transaction costs. Dyhrberg demonstrates how Bitcoin might be viewed similarly to gold, often regarded as a cross between a currency and a commodity [31].

Selgin demonstrated how merchants who have used cryptocurrencies as payment for goods and services have contributed to the steadily rising acceptance rate of Bitcoin [74]. In 2014, the majority of U.S. merchants—more than 75,000 in total—accepted Bitcoin, which also turned out to be a popular way for foreign workers to send money home. In 2012, Selgin emphasised that "the number of merchants embracing Bitcoin at that time had reached about one thousand, and that it was expected to reach ten thousand in another year". He made an effort to highlight the pace at which more and more businesses are taking this cryptocurrency. As of 2020, 36 percent of small and medium-sized enterprises in the United States of America accepted Bitcoin payments, according to specialised websites like 99bitcoins.com. The same website, www.99bitcoins.com, lists several prominent, large businesses that accept Bitcoin, including Wikipedia, KFC, PizzaHut, Overstock, Microsoft, Burger King, Wordpress.com, Reddit, Dell, Target, Expedia, Bloomberg, PayPal, and Tesla Motors, and others [14]. It also emphasises that "almost anything can be bought with Bitcoin today through the use of Bitcoin debit cards,'' issued by Visa or Mastercard. In certain situations, Bitcoin payments are accepted directly, while in others, they are accepted indirectly.

Furthermore, ATMs that allow users to exchange fiat money for Bitcoin have been built in Cyprus, Canada, Romania, and other countries [71]. According to a 2018 study, 2098 Bitcoin ATMs and altcoins are spread across 62 countries [29]. While 2098 is not a large number concerning the total number of ATMs in the world (estimated by The World Bank to be more than 3.5 million in 2020), it does indicate that the existence and use of cryptocurrencies are beginning to be noticed even in this market. While 96 percent of all ATMs are located in North America and Europe, about 60 percent of these ATMs are found in the United States [29]. Just 2.4 percent of ATMs are located in Asia [6].

Demir [27] looks at the connection between the economic policy uncertainty index and Bitcoin and concludes that it can be a useful tool for hedging against uncertainty. However, some studies note that bubbles of speculation and cryptocurrencies' poor intrinsic value contribute to instability and lower price stability. According to Glaser media coverage is a significant factor in determining how volatile cryptocurrency prices are [37]. In terms of stability, it appears that some writers contend that one major drawback of cryptocurrencies is that they lack a central bank to control their supply . Three well-known cryptocurrencies—Bitcoin, Ripple, and Litecoin—and other conventional financial assets—gold, bonds, and others—can be compared to demonstrate how isolated these three cryptocurrencies are from one another and how this can be used to reduce investor risk [22]. Darlington put up an intriguing theory, according to which Bitcoin benefits those who live in developing nations and are experiencing difficulties because it addresses issues with exchange, counterfeiting, and hyperinflation [25].

5 Conclusion

Uses of blockchain technology and cryptocurrencies that are networked by it have shown promise in the banking sector, particularly in the processing of payments and money transfers. This cutting-edge technology still has a great deal of room to grow. With its speed, incredibly low cost, transparency, security, and ease, blockchain technology is most effectively applied in the worldwide money transfer business. The continued adoption of blockchain technology in finance is dependent upon increased familiarity, trust, and confidence generated by a rising number of verified use cases and reviews, as well as suitable regulatory changes.

In this thesis, I offer a thorough analysis of the advancements blockchain technology has brought to the financial industry and will likely continue to do so. To be precise, I concentrated on learning about a few significant applications of blockchain and Bitcoin besides creating a straightforward coin. The mathematical preliminaries portion laid the groundwork for comprehension by clarifying important cryptographic ideas such as symmetric and public-key cryptography, cryptographic protocols, and cryptanalysis. This preparatory work established the framework for assessing the complications associated with transaction security and authentication in decentralised systems The blockchain technology inquiry included an extended analysis of the system's architecture, operation, and wide applications in many economic sectors. In particular, the performance and scalability analysis considered the growing uses of blockchain, solving critical implementation-related challenges. The main findings that have been uncovered during this thesis have been summarised by me. The insights obtained add to my comprehension and suggest future directions for developing cryptocurrency and blockchain technology. By adopting these findings, stakeholders in the industry can direct this cutting-edge technology towards increased effectiveness, sustainability, and societal benefit.

References

[1] Basic block diagram of cryptography. Accessed on November 25, 2023. URL: `https://shorturl.at/ejmK4`.

[2] Latency rate for different blockchain. Accessed on November 25, 2023. URL: `https://shorturl.at/ajvT2`.

[3] Live tps rate of different blockchains. Accessed on November 25, 2023. URL: `https://shorturl.at/uzJR1`.

[4] Mining puzzle demonstration. Accessed on November 25, 2023. URL: `https://shorturl.at/fvBM7`.

[5] Number of bitcoin atms in asia. Accessed on October 29, 2023. URL: `https://www.tzero.com/#what`.

[6] Number of bitcoin atms in asia. Accessed on December 25, 2023. URL: `https://coinatmradar.com/`.

[7] Walmart traces the food product's provenance in seconds. Accessed on November 30, 2023. URL: `https://shorturl.at/mqwGM`.

[8] Omar G Abood and Shawkat K Guirguis. A survey on cryptography algorithms. *International Journal of Scientific and Research Publications*, 8(7):495–516, 2018.

[9] Alaa Hussein Al-Hamami and Ibrahem Abdallah Aldariseh. Enhanced method for rsa cryptosystem algorithm. In *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pages 402–408. IEEE, 2012.

[10] Jameela Al-Jaroodi and Nader Mohamed. Industrial applications of blockchain. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0550–0555. IEEE, 2019.

[11] Simon Albrecht, Stefan Reichert, Jan Schmid, Jens Strüker, Dirk Neumann, and Gilbert Fridgen. Dynamics of blockchain implementation-a case study from the energy sector. 2018.

[12] ES Alu, BO Ahubele, and JT Nnodi. A proposed model for decentralized governance using blockchain technology.

[13] Andreas M Antonopoulos and David A Harding. *Mastering Bitcoin.* O'Reilly Media, Inc, 2023.

[14] Liana Badea and Mariana Claudia Mungiu-Pupzan. The economic and environmental impact of bitcoin. *IEEE Access*, 9:48091–48104, 2021.

[15] Annika Baumann, Benjamin Fabian, and Matthias Lischke. Exploring the Bitcoin Network. *WEBIST (1)*, 2014:369–374, 2014.

[16] Moritz Berneis, Devis Bartsch, and Herwig Winkler. Applications of blockchain technology in logistics and supply chain management—insights from a systematic literature review. *Logistics*, 5(3):43, 2021.

[17] R Bhuvana and PS Aithal. Blockchain based service: A case study on IBM blockchain services & hyperledger fabric. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 4(1):94–102, 2020.

[18] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.

[19] Christian Cachin et al. Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, volume 310, pages 1–4. Chicago, IL, 2016.

[20] Alan Cohn, Travis West, and Chelsea Parker. Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids. *Geo. L. Tech. Rev.*, 1:273, 2016.

[21] CoinMarketCap. Cryptocurrency prices, charts and market capitalizations. 2022.

[22] Shaen Corbet, Brian Lucey, Andrew Urquhart, and Larisa Yarovaya. Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, 62:182–199, 2019.

[23] Gaby G Dagher, Benedikt Bünz, Joseph Bonneau, Jeremy Clark, and Dan Boneh. Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 720–731, 2015.

[24] Jawad Ahmad Dar. Enhancing the data security of simple columnar transposition cipher by caesar cipher and rail fence cipher technique. *International Journal of Computer Science & Engineering Technology (IJCSET)*, 5(11):2229–3345, 2014.

[25] James K Darlington III. The future of bitcoin: Mapping the global adoption of world's largest cryptocurrency through benefit analysis. 2014.

[26] Ruth M Davis, A Konheim, and D Coppersmith. The data encryption standard. In *Proceedings of Conference on Computer Security and the Data Encryption Standard, National Bureau of Standards, Gaithersburg, MD*, pages 500–27, 1977.

[27] Ender Demir, Giray Gozgor, Chi Keung Marco Lau, and Samuel A Vigne. Does economic policy uncertainty predict the bitcoin returns? An Empirical Investigation. *Finance Research Letters*, 26:145–149, 2018.

[28] Whitfield Diffie and Martin E Hellman. New directions in cryptography. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pages 365–390. 2022.

[29] Şerif DİLEK and Yunus Furuncu. Bitcoin mining and its environmental effects. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 33(1):91–106, 2019.

[30] Victor Dostov and Pavel Shust. Cryptocurrencies: An unconventional challenge to the aml/cft regulators? *Journal of Financial Crime*, 21(3):249–263, 2014.

[31] Anne Haubo Dyhrberg. Bitcoin, gold and the dollar–a garch volatility analysis. *Finance Research Letters*, 16:85–92, 2016.

[32] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications.* John Wiley & Sons, 2011.

[33] Dominic Frisby. *Bitcoin: The Future of Money?* Unbound Publishing, 2014.

[34] Ulrich Gallersdörfer, Lena Klaaßen, and Christian Stoll. Energy consumption of cryptocurrencies beyond bitcoin. *Joule*, 4(9):1843–1846, 2020.

[35] Simson Garfinkel. *PGP: Pretty Good Privacy.* O'Reilly Media, Inc., 1995.

[36] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 3–16, 2016.

[37] Florian Glaser, Kai Zimmermann, Martin Haferkorn, Moritz Christian Weber, and Michael Siering. Bitcoin-asset or currency? revealing users' hidden intentions. *Revealing Users' Hidden Intentions (April 15, 2014). ECIS*, 2014.

[38] Evan L Greebel, Kathleen Moriarty, Claudia Callaway, and Gregory Xethalis. Recent key bitcoin and virtual currency regulatory and law enforcement developments. *Journal of Investment Compliance*, 16(1):13–18, 2015.

[39] Tim Güneysu, Timo Kasper, Martin Novotnỳ, Christof Paar, and Andy Rupp. Cryptanalysis with copacobana. *IEEE Transactions on Computers*, 57(11):1498–1513, 2008.

[40] Wolfgang Karl Härdle, Campbell R Harvey, and Raphael CG Reule. Understanding cryptocurrencies, 2020.

[41] Martin E Hellman. An overview of public key cryptography. *IEEE Communications Magazine*, 40(5):42–49, 2002.

[42] Nicolas Houy. The economics of bitcoin transaction fees. *GATE WP*, 1407, 2014.

[43] Md Rafiqul Islam, Muhammad Mahbubur Rashid, Mohammed Ataur Rahman, Muslim Har Sani Bin Mohamad, et al. A comprehensive analysis of blockchain-based cryptocurrency mining impact on energy consumption. *International Journal of Advanced Computer Science and Applications*, 13(4), 2022.

[44] Atul Kahate. Cryptography and network security, 2003, 2006.

[45] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC, 2007.

[46] Ravneet Kaur and Amandeep Kaur. Digital signature. In *2012 International Conference on Computing Sciences*, pages 295–301, 2012. `doi:10.1109/ICCS.2012.25`.

[47] Ashish Kumar Kendhe and Himani Agrawal. A survey report on various cryptanalysis techniques. *International Journal of Soft Computing and Engineering (IJSCE)*, 3(2):287–293, 2013.

[48] Sesha Kethineni and Ying Cao. The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review*, 30(3):325–344, 2020.

[49] Rabiya Khalid, Nadeem Javaid, Sakeena Javaid, Muhammad Imran, and Nidal Naseer. A blockchain-based decentralized energy management in a p2p trading system. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2020.

[50] Leslie Lamport. Paxos made simple. *ACM SIGACT News (Distributed Computing Column) 32, 4 (Whole Number 121, December 2001)*, pages 51–58, 2001.

[51] Noureddine Lasla, Lina Al-Sahan, Mohamed Abdallah, and Mohamed Younis. Green-pow: An energy-efficient blockchain proof-of-work consensus algorithm. *Computer Networks*, 214:109118, 2022.

[52] Steven Levy. *Crypto: How the code rebels beat the government–saving privacy in the digital age*. Penguin, 2001.

[53] AG Luchkin, OL Lukasheva, NE Novikova, VA Melnikov, AV Zyatkova, and EV Yarotskaya. Cryptocurrencies in the global financial system: Problems and ways to overcome them. In *Russian Conference on Digital Economy and Knowledge Management (RuDEcK 2020)*, pages 423–430. Atlantis Press, 2020.

[54] Michael Mainelli and Chiara Von Gunten. Chain of a lifetime: How blockchain technology might transform personal insurance. *How Blockchain Technology Might Transform Personal Insurance-Long Finance*, 2014.

[55] Akash Kumar Mandal, Chandra Parakash, and Archana Tiwari. Performance evaluation of cryptographic algorithms: Des and aes. In *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, pages 1–5, 2012. `doi:10.1109/SCEECS.2012.6184991`.

[56] James L Massey. Cryptography—a selective survey. *Digital Communications*, 85:3–25, 1986.

[57] Daniela Mechkaroska, Vesna Dimitrova, and Aleksandra Popovska-Mitrovikj. Analysis of the possibilities for improvement of blockchain technology. pages 1–4, 11 2018. `doi:10.1109/TELFOR.2018.8612034`.

[58] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. A review on consensus algorithm of blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 2567–2572, 2017. `doi:10.1109/SMC.2017.8123011`.

[59] Vijay Kumar Mitali, Arvind Sharma, et al. A survey on various cryptography techniques. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 3(4):307–312, 2014.

[60] B Bazith Mohammed. Automatic key generation of caesar cipher. *Int. J. Eng. Trends Technol*, 6(6):2231–5381, 2013.

[61] Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17*, pages 25–33. Springer, 2013.

[62] Debdeep Mukhopadhyay and BA Forouzan. Cryptography and network security. *Noida: Tata Mcgraw Hill*, 2011.

[63] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 2008.

[64] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies. *Curso Elaborado Pela*, 1(1):1–308, 2021.

[65] Tingyuan Nie and Teng Zhang. A study of DES and blowfish encryption algorithm. In *TENCON 2009 - 2009 IEEE Region 10 Conference*, pages 1–4, 2009. `doi:10.1109/TENCON.2009.5396115`.

[66] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. *Business & Information Systems Engineering*, 59:183–187, 2017.

[67] Ritu Patidar and Rupali Bhartiya. Modified RSA cryptosystem based on offline storage and prime number. In *2013 IEEE International Conference on Computational Intelligence and Computing Research*, pages 1–6. IEEE, 2013.

[68] Harsha V Patil, Kanchan G Rathi, and Malati V Tribhuwan. A study on decentralized e-voting system using blockchain technology. *Int. Res. J. Eng. Technol*, 5(11):48–53, 2018.

[69] Giulio Prisco. The blockchain for healthcare: Gem launches gem health network with philips blockchain lab. *Bitcoin Magazine*, 26, 2016.

[70] Vincent Rijmen and Joan Daemen. Advanced encryption standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, 19:22, 2001.

[71] Angela Rogojanu, Liana Badea, et al. The issue of competing currencies. case study–bitcoin. *Theoretical and Applied Economics*, 21(1):103–114, 2014.

[72] Abdurrashid Ibrahim Sanka and Ray CC Cheung. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications*, 195:103232, 2021.

[73] Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, 62(6):599–608, 2020.

[74] George Selgin. Bitcoin: Problems and prospects. 2022.

[75] Gurpreet Singh. A study of encryption algorithms (rsa, des, 3des and aes) for information security. *International Journal of Computer Applications*, 67(19), 2013.

[76] Simar Preet Singh and Raman Maini. Comparison of data encryption algorithms. *International Journal of Computer Science and Communication*, 2(1):125–127, 2011.

[77] E Thambiraja, G Ramesh, and Dr R Umarani. A survey on various most common encryption techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(7), 2012.

[78] Stallings William. Network security essentials: Applications and standards. *Pearson Education, Inc., Publishing as Prentice Hall*, 1:77–78, 2000.

[79] Di Yang, Chengnian Long, Han Xu, and Shaoliang Peng. A review on scalability of blockchain. In *Proceedings of the 2020 the 2nd International Conference on Blockchain Technology*, pages 1–6, 2020.

[80] Peng Zhang and Maged N Kamel Boulos. Blockchain solutions for healthcare. In *Precision Medicine for Investigators, Practitioners and Providers*, pages 519–524. Elsevier, 2020.

[81] Peng Zhang, Jules White, and Douglas Schmidt. Architectures and patterns for leveraging high-frequency, low-fidelity data in the healthcare domain. In *2018 IEEE International Conference on Healthcare Informatics (ICHI)*, pages 463–464. IEEE, 2018.

[82] Peng Zhang, Jules White, Douglas C Schmidt, Gunther Lenz, and S Trent Rosenbloom. Fhirchain: Applying blockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal*, 16:267–278, 2018.

[83] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564. IEEE, 2017.